Kingdom of Saudi Arabia
Ministry of Interior
High Commission for Industrial Security
Secretariat General

المملكة العربية السعودية
وزارة الداخلية
الهيئة العليا للأمن الصناعي
الأمانة العامة

SECURITY DIRECTIVES FOR INDUSTRIAL FACILITIES



نسخة مرخصة لـ [illegible]

2017 ISSUE

نسخة مرخصة لـ شركة المياه الوطنية

INTRODUCTION

The national security of Saudi Arabia, including the security of the economy and the well-being of its population, depends directly on the physical and operational safety of a range of facilities across Saudi Arabia. These facilities are required to have adequate levels of protection as defined within these Directives.

The High Commission for Industrial Security, referred to as HCIS, is the national regulatory agency for Security, Safety & Fire Protection requirements at industrial facilities and designated critical infrastructure, Kingdom-wide. The HCIS Security Directives are mandated by the Minister of Interior, Kingdom of Saudi Arabia. The HCIS issues the Security, Safety & Fire Protection directives.

These Directives set forth the framework under which HCIS specifies safety, fire protection and security requirements at the facilities under its jurisdiction. Facility operators are responsible for compliance with the regulations stated therein.

Compliance with these Directives is a statutory requirement under the laws of the Kingdom of Saudi Arabia. Failure to comply with HCIS regulations at facilities under HCIS jurisdiction may result in operation delays as HCIS approvals are a prerequisite for facility operation.

HCIS reserves the exclusive right to modify, add to, or amend, the Security, Safety & Fire Protection Directives without prior notice.

نسخة مرخصة لـ شركة المياه الوطنية

Kingdom of Saudi Arabia
Ministry of Interior
High Commission for Industrial Security
Secretariat General

المملكة العربية السعودية
وزارة الداخلية
الهيئة العليا للأمن الصناعي
الأمانة العامة

LIST OF SECURITY (SEC) DIRECTIVES

SEC#	*SEC TITLE*
SEC-01	*General Requirements for Security Directives*
SEC-02	*Security Fencing Systems*
SEC-03	*Security Gates*
SEC-04	*Security Lighting*
SEC-05	*Security Systems at Industrial Facilities*
SEC-06	*Security Devices*
SEC-07	*Power Supplies*
SEC-08	*Security Communications & Data Networks*
SEC-09	*Structures Housing Security Equipment **
SEC-10	*Railway Operations in Industrial Facilities**
SEC-11	*Personal Identification Verification Cards*
SEC-12	*Cybersecurity*
SEC-13	*Facilities with Marine Interface **
SEC-14	*Security Project Management**
SEC-15	*Security Management at Industrial Facilities **
SEC-16	*Pipeline & Pipeline Corridors **
SEC-17	*Electrical Power Substations **
SEC-18	*Security for Industrial Cities**
SEC-19	*Residential Compounds for Industrial Facilities **

(*) New SECs

نسخة من خدمة تشريعات الوطنية

نسخة مرخصة لـ شركة المياه الوطنية

SEC-01

General Requirements for Security Directives

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7

2 SCOPE 7

3 ACRONYMS & DEFINITIONS 8

4 REFERENCES 8

5 AUTHORITY 9

6 APPLICATION 9

7 WAIVERS 10

8 FACILITY SECURITY CLASSIFICATION 11

8.1 General 11
8.2 Business Criteria Analysis 11
8.3 Security Risk Assessment 12

9 MATERIALS AND EQUIPMENT 13

10 NON-DISCLOSURE AGREEMENT 13

11 ENVIRONMENTAL REQUIREMENTS 13

11.1 Indoor Environment 13
11.2 Outdoor Environment 13

12 SECURITY PROJECTS 15

12.1 Security Project Service Providers 15
12.2 HCIS Approval Stages 16
12.3 Security Project Submission Requirements 16

13 FACILITY SECURITY PLAN 17

14 USAGE OF PORTABLE ELECTRONIC DEVICES IN RESTRICTED AREAS 17

15 PROOF OF COMPLIANCE 18

APPENDIX-A: FACILITY SECURITY CLASSIFICATION 19

APPENDIX-B: BUSINESS CRITERIA ANALYSIS (BCA) WORKSHEET 23

APPENDIX-C: CLASS 5 REQUIREMENTS 26

نسخة مرخصة لشركة الميادين الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document provides general and administrative requirements for implementing the Security Directives (SEC) listed under Section 2.

2 Scope

This directive provides Facility Operators (FO) with the general requirements for implementing the SEC directives at facilities under the jurisdiction of the HCIS.

The contents of this directive apply to the following SECs:

SEC-01:	General Requirements for Security Directives
SEC-02:	Security Fencing
SEC-03:	Security Gates
SEC-04:	Security Lighting
SEC-05:	Security Systems at Industrial Facilities
SEC-06:	Security Devices
SEC-07:	Power Supply
SEC-08:	Security Communications & Data Networks
SEC-09*:	Structures Housing Security Equipment
SEC-10*:	Railway Operations in Industrial Facilities
SEC-11:	Personal Verification Identification Cards
SEC-12:	Cyber Security
SEC-13*:	Facilities with Marine Interface
SEC-14*:	Security Project Management
SEC-15*:	Security Operations at Industrial Facilities
SEC-16*:	Pipelines & Pipeline Corridors
SEC-17*:	Electrical Power Substations
SEC-18*:	Security for Industrial Cities
SEC-19*:	Residential Compounds for Industrial Facilities

** Initial issue 2016*

These directives refer to Safety & Fire Protection directives (SAF) also issued by HCIS.

نسخة من خصيصاً لشركة الهيئة الوطنية

3 Acronyms & Definitions

AHJ	Authority Having Jurisdiction
BCA	Business Criteria Analysis
FC	Functional Classification
FO	Facility Operator: the owner, operator or lessee of a facility
FSC	Facility Security Classification
FSP	Facility Security Plan
HCIS	High Commission for Industrial Security
HCIS RI	The Regulatory Instructions for Industrial Security in Petroleum, Industrial, Service Companies and Institutions that are Supervised by the High Commission for Industrial Security (HCIS). Issued by HCIS 1430H/2009
SAF	Safety & Fire Protection Directives
SEC	Security Directives
SRA	Security Risk Assessment
Shall	Indicates a mandatory requirement
Should	Indicates an advisory requirement

4 References

The current versions of the references in each SEC directive shall be applicable. They shall be considered integral to the SEC Directives.

ANSI/API/STD 780	*American Petroleum Institute (API) - Standard 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, First Edition, March 2013.*
CCPS	*Center for Chemical Process Safety (CCPS), Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*
ASIS RA	*ASIS International: Risk Assessment Standard ANSI/ASIS/RIMS RA.1-2015*
SAF-12	*Electrical Safety*
SAF-19	*Power Plants and Associated Facilities*
SEC-14	*Security Project Management*
SEC-15	*Security Management at Industrial Facilities*
SEC-17	*Electrical Power Substations*

5 Authority

HCIS has the authority to modify SEC directives without prior notice and to act as the AHJ for the implementation of SECs for infrastructures deemed critical and for facilities in the following sectors:

- Petroleum
- Electric Power & Distribution
- Petrochemical
- Water
- Industrial Services
- Communications
- Mining
- Gas
- Civil Explosives
- Chemical Manufacturing
- Metal Manufacturing
- Ports
- Railroads
- Others as determined by HCIS

6 Application

6.1 Application of Security Directives

6.1.1 SEC directives shall be applied throughout the lifecycle of relevant facilities. This includes planning, design, construction, commissioning, operations, maintenance, modifications, upgrades and decommissioning.

6.1.2 This Directive is applicable to all facilities including existing facilities, the expansion of existing facilities, new facilities, projects, and upgrades.

6.1.3 The HCIS reserves the right to modify and/or make changes, as deemed necessary, to the Security Directives without prior notice.

6.1.4 FO is responsible for full compliance with HCIS requirements. Any deficiencies detected during an HCIS inspection of the facility shall be corrected at FO's expense.

نسخة مرخصة لشركة المياه الوطنية

6.2 Compliance

6.2.1 All existing facilities shall comply with these directives within 2 years from the release date of these directives.

6.2.2 Where FO can demonstrate that the existing facility physical security infrastructure is compliant with the previous directives then the facility shall be exempt from 6.2.1 until an upgrade, expansion or replacement of the security infrastructure is required.

6.2.3 All new facilities shall fully comply with these directives.

7 Waivers

7.1 Internal Company Standards

7.1.1 These directives supersede all Directives previously issued by the HCIS, or with any other standard.

7.1.2 The FO shall align its internal standards with SEC directives.

7.2 Waiver Requests

7.2.1 The FO shall seek specific approval from HCIS for any non-compliance with SEC Directives.

7.2.2 Any request for non-compliance shall be submitted to HCIS with justification proving that the non-compliances, and their resolutions, meets or exceeds SEC Directive requirements.

7.2.3 Waiver requests shall be based on the non-compliances identified during the SRA stage, the risk mitigation & countermeasure recommendations, sound engineering reasons and justifications.

In order to request a waiver, the FO shall submit a formal request to HCIS containing the following:

7.2.3.1. Facility location
7.2.3.2. Project details
7.2.3.3. Security Directive section/paragraph that is being impacted
7.2.3.4. Waiver description
7.2.3.5. Non-compliance risk impact
7.2.3.6. Reason for waiver request
7.2.3.7. Alternatives that have been considered

نسخة مرخصة لشركة المياه الوطنية

7.2.3.8. Risk mitigation strategy if the waiver is implemented

7.2.3.9. Relevant drawings that illustrate the details of the request

8 Facility Security Classification

8.1 General

8.1.1 The baseline security requirements definitions for a facility shall be based on its FSC.

8.1.2 Facilities shall be classified based on a five (5) level classification methodology with Class 1 being the highest level and Class 5 being the lowest level.

8.1.3 The business criteria for determining the FSC of a specific facility are defined in Appendix A.

8.1.4 Electrical substations and water pumping & storage facilities do not fit into the regular FSC criteria for facilities and their security requirements definitions are based on a Functional Classification (FC).

The details for the FC of Electrical Substations are in SEC-17 “Electrical Power Substations”.

8.1.5 HCIS reserves the exclusive right to determine the final FSC for a facility.

8.2 Business Criteria Analysis

8.2.1 The FO shall conduct a BCA to determine how the facility parameters match the business criteria specified in Appendix-A. This analysis shall be presented in the form of a Business Criteria Worksheet as shown in Appendix-B.

8.2.2 Each facility under the jurisdiction of HCIS shall have a FSC assigned based on the BCA.

8.2.3 Each criterion shall be addressed and its applicability to the facility in question shall be detailed so that the basis of the FSC recommendation can be evaluated by HCIS.

8.2.4 The FO shall complete this worksheet, with specific information and supporting documents, that addresses each applicable criterion.

8.3 Security Risk Assessment

8.3.1 The Security Risk Assessment (SRA) shall be executed by a HCIS approved Security Consultant as specified in SEC-15.

8.3.2 The FO shall conduct a SRA for the facility as specified below:

8.3.2.1. An initial assessment of the facility to formulate the baseline security requirement.

8.3.2.2. When the commissioning of a new facility is completed an SRA shall be conducted as follows:

- For Class 1 facilities 1 per year with follow-up meeting.
- For Class 2 facilities 1 per year.
- For Class 3 & 4 facilities 1 every 18 months.

8.3.2.3. When a new process or operation is proposed that may impact the existing security posture or as recorded by the latest SRA recommendations.

8.3.2.4. Expansion of existing facilities or any change in the physical layout of the facility that impacts the perimeter or gates.

8.3.2.5. When the threat substantially changes, at the discretion of the FO or when directed by HCIS.

8.3.2.6. After a significant security incident.

8.3.3 The SRA shall incorporate the requirements stated in SEC-15.

8.3.4 The FO shall be responsible to ensure that the SRA shall be executed in accordance with any of the following SRA methodologies or standards:

8.3.4.1. American Petroleum Institute (API) - Standard 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, First Edition, March 2013.

8.3.4.2. Center for Chemical Process Safety (CCPS), Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites.

8.3.4.3. ASIS International: Risk Assessment Standard ANSI/ASIS/RIMS RA.1-2015.

9 Materials and Equipment

The selection of material and equipment, the design, construction, maintenance, operation, repair of equipment and facilities covered by this SEC directive shall comply with the latest edition of the references listed in each SEC directive, unless otherwise noted.

10 Non-Disclosure Agreement

Companies involved in projects shall sign Non-Disclosure Agreements stating that no document shall be disclosed to a third party without prior written approval of FO.

11 Environmental Requirements

11.1 Indoor Environment

11.1.1 All security equipment and rooms or cabinets housing security equipment shall be cooled, or heated as necessary, with redundant split or central air-conditioning units.

11.1.2 Security equipment installed in cabinets shall use a cabinet specific air-conditioner.

11.1.3 Window type air conditioners shall not be used for cooling any security facilities or equipment.

11.2 Outdoor Environment

11.2.1 Security equipment that is installed outdoors shall be rated to operate in direct sunlight under the environmental conditions stated below to ensure that reliable equipment function:

11.2.1.1. Ambient Temperature Range:
-10°C to +60°C in direct sunlight[1,2]

11.2.1.2. Ambient Relative Humidity Range:
5% to 95%, non-condensing

11.2.1.3. Airborne dust concentration:
Annual Average: 0.3 mg/m
Sandstorm: 3 mg/m

11.2.1.4. Wind Speed: 112 km/hour

11.2.1.5. Other Pollutants (vol/vol)
CO: 50 ppm
H_2S: 10 ppm
Hydrocarbons: 150 ppm
NOx: 5 ppm
O^3: 1 ppm
SO^2: 10 ppm

11.2.2 Equipment to be installed outdoor shall be designed to operate without air conditioning or forced air ventilation system and under the environmental conditions listed above and shall meet listed performance when subjected to the full range of these conditions.

نسخة من خصة شركة الدراية الوطنية

[1] *Excluding temperature rise in cabinet*

[2] *Lower temperature rated equipment may be used when FO can demonstrate the maximum temperature encountered over the last 20 years is lower than 60°C or higher then -10°C. The historical temperature data must be provided from a source certified by the Saudi Government Presidency of Meteorology and Environment.*

11.2.3 Equipment that is not capable of operating in such temperatures shall be installed in a cabinet with active cooling specifically designed for the cabinet. The contractor shall provide certification, by an independent authority, that the cabinet is rated for operation in the conditions specified in this section.

11.2.4 Equipment designated for outdoor usage shall be certified by an independent internationally recognized authority as being fully compliant with the standards and specifications stipulated on the equipment data sheet.

11.2.5 The FO shall ensure that the SRA for the facility include an analysis of the average environmental conditions applicable to the specific facility.

12 Security Projects

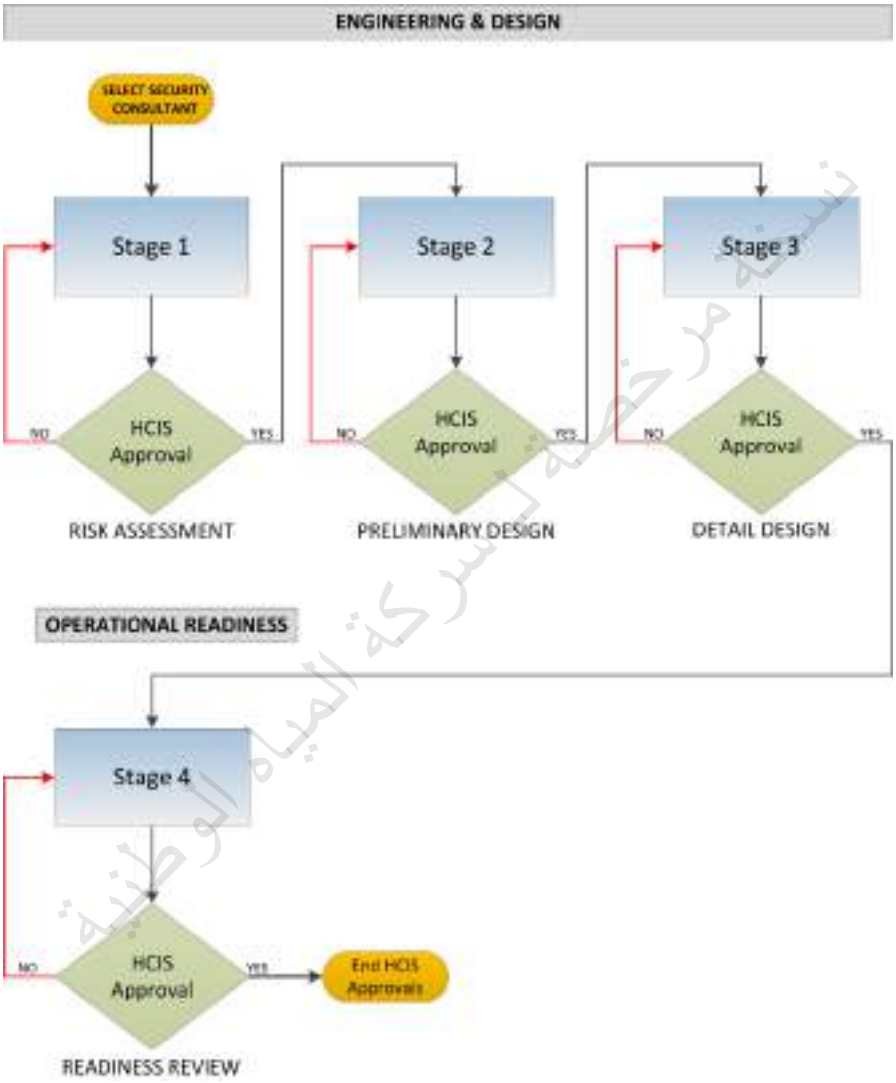
12.1 Security Project Service Providers

Only HCIS approved security consultants and contractors shall work on the security infrastructure, security system design, and implementation of SEC compliant requirements for facilities. Refer to section 5.2, SEC-14 for further details.

نسخة مرخصة لشركة المياه الوطنية

12.2 HCIS Approval Stages

Security Projects shall follow a 4 stage HCIS approval process as shown in the diagram below. The details for each stage are stipulated in SEC-14.



12.3 Security Project Submission Requirements

12.3.1 The prerequisite for starting the HCIS project approval workflow is the selection of a security consultant as specified in section 12.1 & SEC-14.

12.3.2 FSC recommendation and Business Criteria Analysis Worksheet shall be submitted during Stage 1 as part of the SRA.

13 Facility Security Plan

All facilities shall develop and implement an FSP to manage facility security during development, design, construction and operations. The details for the FSP are stipulated in SEC-15.

14 Usage of Portable Electronic Devices in Restricted Areas

Usage of portable electronic devices in restricted areas shall fully comply with the requirements of SAF-12, section 7.4. Additionally, FO shall develop a policy, from the security perspective, to address the usage of such devices within a facility which may preclude their usage in selected areas.

نسخة مرخصة لشركة المياه الوطنية

15 Proof of Compliance

15.1 General Requirements

FO shall validate compliance with all SEC directive requirements by submitting Proof of Compliance (PoC) during facility security surveys, as specified in SEC-01, 8.3.2 and any security related project design activity as specified in SEC-14. Each directive contains specific PoC requirements that must be submitted with the SRA and any project submission. The PoC for each directive shall form part of the normal submission documentation and shall not be duplicated or included as additional documentation.

15.2 SEC-01 PoC

FO shall provide HCIS with a SEC-01 specific Proof of Compliance (PoC) as part of the workflow (as specified), to demonstrate how the FO is complying with specific requirements in this directive.

This PoC shall provide the details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-01 Reference	Requirement	FO Response
1.	7	Waivers[1]	*Submit all waivers as specified in section 7*
2.	8.2	FSC[2]	*Submit BCA*
3.	8.3	SRA[2]	*Submit SRA*
4.	11	Environmental[1]	*Submit catalogs and certifications proving environmental rating compliance*

1: Stage 3 or earlier submission
2: Stage 1 submission

APPENDIX-A: FACILITY SECURITY CLASSIFICATION

1 Class 1 Facility

A Class 1 facility is defined as any facility whose destruction, or serious damage, could seriously damage the Kingdom's economy or gravely disrupt the well-being of its population.

Such facilities are characterized by meeting ANY of the following criteria in the event of their damage or destruction:

Business Criteria

- Serious impact to offsite & onsite population due to large-scale toxic or flammable release.
- Major environmental impact onsite and/or offsite areas.
- Very large capital investment.
- Very long term business interruption with large-scale disruption to the national economy or loss of critical data.
- Critical infrastructure, regardless of capital investment or availability of alternates.
- Other critical national infrastructure is dependent on this facility's outputs, products or services.
- Loss of function/capacity cannot be made up by other existing facilities.
- Directly and seriously impacts hydrocarbon exports.

The following facilities are examples of Class 1 facilities:

- Major oil & gas production, processing, transportation & export facilities including Gas Oil Separator Plants (GOSP).
- Major oil refining & storage.
- Hydrocarbon plants.
- Major electricity generation facilities.
- Major water desalination facilities.
- Major commercial & industrial sea ports including all hydrocarbon export seaports.
- Major telecommunications facilities.

نسخة مرخصة لشركة المياه الوطنية

- Major facilities using or producing chemicals whose flammability, explosiveness, toxicity and evaporability may cause serious harm to the environment or population if the facility is damaged or destroyed.
- Manufacturing & storage facilities for commercial explosives and all other explosive storage facilities.
- Infrastructure that supports, or contains facilities or services, that are deemed important to the national interest.
- Bulk plants.

2 Class 2 Facility

A Class 2 facility is defined as any facility whose destruction, or serious damage, could cause short term damage to the Kingdom's economy or temporarily disrupt the well-being of its population.

Such facilities are characterized by meeting ANY of the following criteria in the event of their damage or destruction:

Business Criteria

- Serious impact on onsite personnel & possibility of offsite injuries or casualties.
- Very large environmental impact onsite and/or offsite areas.
- Medium capital investment.
- Long term business interruption.
- Loss of function/capacity can be compensated for short periods by other existing facilities.
- Directly impacts hydrocarbon exports but will not significantly reduce them.

The following facilities are examples of Class 2 facilities:

- Minor facilities for hydrocarbon production, processing, transportation & export.
- Facilities using or producing chemicals whose relatively low flammability, explosiveness, toxicity and evaporability present medium level risk to the environment or population if the facility is damaged or destroyed.
- Major pumping facilities for oil and water.
- Major computer facilities that manage the above items.

نسخة مرخصة لشركة الأمن الوطنية

3 Class 3 Facility

A Class 3 facility is defined as any facility whose disruption, or serious damage, could cause minimal or no damage to the Kingdom's economy or would not disrupt the well-being of its population.

Such facilities are characterized by meeting ANY of the following criteria in the event of their damage or destruction:

Business Criteria

- Possibility of onsite injuries or casualties with no offsite impact.
- Environmental impact onsite and/or minor impact in offsite areas.
- Small capital investment.
- Medium term business interruption.
- Loss of function/capacity can be compensated for an extended period by other existing facilities.
- No direct impact on oil exports.

The following facilities are examples of Class 3 facilities:

- Minor sea ports.
- Low capacity electricity generation.
- Minor telecommunications facilities.

4 Class 4 Facility

A Class 4 facility is defined as any facility considered a facility that supports a class 1, 2 or 3 facility and is either adjacent to, or remote to, Class 1, 2 or 3 facilities.

Business Criteria

Such facilities are characterized by meeting ANY of the following criteria:

- Possibility of localized onsite casualties or injuries with no offsite impact.
- Minor environmental impact to immediate incident area.
- Minimal capital investment.
- Short term business interruption.

نسخة مرخصة لشركة المدينة الوطنية

The following facilities are examples of Class 4 facilities:

- Supply warehouses.
- Office support facilities.

5 Class 5 Facility

A Class 5 facility is defined as an industrial facility that has no economic or environmental impact on the Kingdom or its population and is not located adjacent to critical national infrastructure.

Class 5 is very limited in its application and shall only be assigned by HCIS.

Business Criteria

- Possibility of minor onsite casualties or injuries with no offsite impact.
- No environmental impact.
- Very short term business interruption.
- Facility is located within secondary industrial areas of the Kingdom.
- Does not directly support a Class 1, Class 2 or a Class 3 facility.

Limitations:

- Assignment of Class 5 is solely at HCIS discretion.
- Facility operator shall be required to characterize all possible environmental risks as a pre-requisite for classification as Class 5.

Workflow

Facilities classified as Class 5 shall follow a simplified workflow as detailed in Appendix C of this directive.

نسخة مرخصة لـ شركة المياه الوطنية

APPENDIX-B: BUSINESS CRITERIA ANALYSIS (BCA) WORKSHEET

Business Criteria Analysis - Worksheet

- Facility Operators (FO) shall fill in this worksheet to provide specific details on what does, or does not, apply to a facility that is being reviewed for its Facility Security Classification (FSC) as specified in SEC-01.
- Under FO Response, fill in either Yes or No. If No is entered then provide details on why the criteria is not applicable.
- Filling in Yes in any criteria identifies the Facility Security Classification.

	Criteria	FO Response (Y/N)	FO Response Details
	CLASS 1		
1.	Serious impact to offsite & onsite population due to large-scale toxic or flammable release		*Specify processes & chemicals used at the facility and why they do, or do not, present a serious impact to offsite & onsite population*
2.	Major environmental impact onsite and/or offsite areas		*Specify potential environmental impact due to processes and materials used at the facility if they are catastrophically damaged*
3.	Very large capital investment		*Specify how this facility's replacement cost relates to the overall company annual budget and approximately in what percentile does it fall in a table of facilities and their related costs.* *Example: 750 million USD, 45% cost percentile*
4.	Very long term business interruption with large-scale disruption to the national economy or loss of critical data		*What is the impact of the loss of this facility on the national economy?* *What critical data shall be lost?*
5.	Critical infrastructure, regardless of capital investment or availability of alternates		*If this is applicable, specify how it applies.*
6.	Other critical national infrastructure is dependent on this facility's outputs, products or services		*What other major facilities or critical national infrastructure is dependent on this facility's output, products or services?*
7.	Loss of function/capacity cannot be made up by other existing facilities		*Specify what facilities will make up the function or capacity of this facility*
8.	Directly and seriously impacts hydrocarbon exports		*What percentage of Hydrocarbon exports shall be impacted?*

CONFIDENTIAL

Business Criteria Analysis - Worksheet

	CLASS 2		
1.	Serious impact on onsite personnel & possibility of offsite injuries or casualties		*Specify processes & chemicals used at the facility and why they do, or do not, not present a serious impact to offsite & onsite population*
2.	Very large environmental impact onsite and/or offsite areas		*Specify potential environmental impact due to processes and materials used at the facility if they are catastrophically damaged*
3.	Medium capital investment		*Specify how this facility's replacement cost relates to the overall company annual budget and approximately in what percentile does it fall in a table of facilities and their related costs.* *Example: 750 million USD, 45% cost percentile*
4.	Long term business interruption		*What is the impact of the loss of this facility on the owner, operator or lessee?*
5.	Loss of function/capacity can be compensated for short periods by other existing facilities		*Specify what facilities will make up the function or capacity of this facility*
6.	Directly impacts hydrocarbon exports but will not significantly reduce them		*What percentage of Hydrocarbon exports shall be impacted?*

	CLASS 3		
1.	Possibility of onsite injuries or casualties with no offsite impact		*Specify processes & chemicals used at the facility and why they do, or do not, not present a serious impact to offsite & onsite population*
2.	Environmental impact onsite and/or minor impact in offsite areas		*Specify potential environmental impact due to processes and materials used at the facility if they are catastrophically damaged*
3.	Small capital investment		*Specify how this facility's replacement cost relates to the overall company annual budget and approximately in what percentile does it fall in a table of facilities and their related costs.* *Example: 750 million USD, 45% cost percentile*
4.	Medium term business interruption		*What is the impact of the loss of this facility on the owner, operator or lessee?*
5.	Loss of function/capacity can be compensated for an extended period by other existing facilities		*If this is applicable, specify how it applies.*

CONFIDENTIAL

Business Criteria Analysis - Worksheet

6.	No direct impact on oil exports		*What percentage of Hydrocarbon exports shall be impacted?*

CLASS 4			
1.	Possibility of localized onsite casualties or injuries with no offsite impact		*Specify processes & chemicals used at the facility and why they do, or do not, not present a serious impact to offsite & onsite population*
2.	Minor environmental impact to immediate incident area		*Specify potential environmental impact due to processes and materials used at the facility if they are catastrophically damaged*
3.	Minimal capital investment		*Specify how this facility's replacement cost relates to the overall company annual budget and approximately in what percentile does it fall in a table of facilities and their related costs.* *Example: 750 million USD, 45% cost percentile*
4.	Short term business interruption.		*What is the impact of the loss of this facility on the owner, operator or lessee?*

CLASS 5			
1.	Possibility of minor onsite casualties or injuries with no offsite impact		*Specify processes & chemicals used at the facility and why they do, or do not, not present a serious impact to offsite & onsite population*
2.	No environmental impact		*Specify potential environmental impact due to processes and materials used at the facility if they are catastrophically damaged*
3.	Very short term business interruption		*What is the impact of the loss of this facility on the owner, operator or lessee?*
4.	Facility is located within secondary industrial areas of the Kingdom		*Specify location of facility & confirm it is in secondary areas*
5.	Does not directly support a Class 1, Class 2 or a Class 3 facility		*What facilities are supported by the output, products or services of this facility?*

CONFIDENTIAL

APPENDIX-C: CLASS 5 REQUIREMENTS

1. PERIMETER FENCING

   a. Solid walls along the perimeter are not permitted unless required due to safety requirements. Such solid perimeter walls shall be limited to the sections of the perimeter where the safety requirement applies.

      Facility operator shall provide HCIS with applicable safety references that are being used as the basis for this aspect.

   b. The perimeter fencing may be rigid steel fencing or chain-link, as selected by the facility operator, with the following physical attributes:
      i. Fence design shall be selected to allow clear views into the facility from the outside.
      ii. 3m height minimum.
      iii. Topped by one roll of properly secured concertina wire.
      iv. All fence components shall be protected against corrosion by the appropriate coatings.
      v. Clear zones on both sides of the fence. This clear zone shall be graded and kept clear of all vegetation. Facility operator shall not use these areas for any purpose.
      vi. 3m clear zone on the outside.
      vii. 2m clear zone on the inside.

2. GATE

   a. Guardhouse - a permanent structure with ballistic protection.
   b. Auxiliary gate.
   c. Raise arm barrier.
   d. Access Control system. All vehicle and pedestrian lanes.
   e. Appropriate fencing to force all personnel through the access control system.
   f. Adequate lighting in gatehouse area to inspect vehicles, personnel and documents.

3. LIGHTING

   a. Area/street lighting shall be used along the perimeter fence and main roadways inside the facility.
   b. All buildings shall have lighting illuminating the building exterior.
   c. Lighting shall be automatically on during periods of darkness.

4. PROCEDURES

   a. Facility operator shall develop and implement procedures for each guard post.
   b. Security personnel shall be trained in the use of all security equipment used at the facility.
   c. Security personnel shall have adequate wireless communication resources to cover the entire facility.
   d. Selection of security personnel shall follow HCIS regulations.
   e. ID management system.
   f. Visitor management system.

5. IMPLEMENTATION

   a. Facility operator shall submit a report to HCIS characterizing all possible environmental risks at the facility and how it complies with Class 5 criteria.
   b. HCIS shall provide facility operator with one of the following:
      i. Confirm classification as Class 5.
      ii. Require facility operator to be classified higher. This will require compliance with SEC-01 "*General Requirements for Industrial Security*".
   c. Facilities classified as Class 5 may proceed with their internal design process, in compliance with the above requirements and using a contractor of their own selection.
   d. Facility operator shall inform HCIS of the commissioning of the facility security system.
   e. Facility operator is responsible for full compliance with HCIS requirements in this, and other applicable SEC Directives. Any deficiencies detected during an HCIS inspection of the facility shall be corrected at the facility operator's expense.

نسخة من الهيئة العليا للأمن الصناعي

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-02

Security Fencing System

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7

2 SCOPE 7

3 ACRONYMS & DEFINITIONS 7

4 REFERENCES 8

5 GENERAL REQUIREMENTS 9

5.1 Introduction 9
5.2 Fence Definition Methodology 10
5.3 Category 1 Fencing System 12
5.4 Category 2 Fencing System 14
5.5 Category 3 Fencing System 16
5.6 Category 4 Fencing System 17
5.7 Category 5 Fencing System 18
5.8 Shared Fencing between Adjacent Facilities 18
5.9 Internal Separation Fence 20
5.10 Construction Fence 20
5.11 Outer Property Fence 21
5.12 Clearances 21

6 DESIGN REQUIREMENTS 22

6.1 Anti-Vehicle Barrier 22
6.2 Structural Performance 22
6.3 Durability Performance 23
6.4 Forced Entry Resistance Performance 23
6.5 Fence Fabric & Panels 24
6.6 Visibility Index (VI) 24
6.7 Razor Tape 25
6.8 Barbed Wire 25
6.9 Tie Wire 26
6.10 Concrete 26
6.11 Grounding 26
6.12 Alignment & Terrain Profiling 27
6.13 Post Installation Requirements 28
6.14 Chain Link Specific Requirements 28
6.15 Rigid Welded Mesh Specific Requirements 30
6.16 Fence Penetration 31
6.17 Emergency Gates 33

7 APPLICATION OF REQUIREMENTS 34

8 PROOF OF COMPLIANCE 35

نسخة من نصه لشركة المباني الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document provides requirements for fencing systems at a facility perimeter.

2 Scope

This directive includes the layout of the various categories of fencing systems, different types of fences and the design requirements for fences.

3 Acronyms & Definitions

AVB	Anti-Vehicle Barrier: There are three types of AVB: • Deployable AVB: *This type of AVB is deployed at gates in the vehicle traffic lanes & is commonly referred to as a* Road Blocker. • Fixed AVB: *This type of AVB is deployed as part of the perimeter fencing system.* • Bollards: *Bollards may be fixed or deployable. They are required for traffic management and roadway containment in the gate area.*
CCTV	Close Circuit Television
CL	Chain Link
FDC	Field Distribution Cabinet
FO	Facility Operator: the owner, operator or lessee of a facility
FSC	Facility Security Classification
HCIS	High Commission for Industrial Security
IDAS	Intrusion Detection Assessment System
LRS	Long Range Surveillance System
PTZ	Pan-Tilt-Zoom
PVC	Polyvinyl Chloride
RWM	Rigid Welded Mesh
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory requirement
VASS	Video Assessment & Surveillance System
VI	Visibility Index

نسخة من الهيئة العليا للأمن الصناعي

4 References

This directive adopts the latest edition of the references listed.

The selection of material and equipment, and the design, construction, maintenance, operation and repair of equipment and facilities covered by this SEC directive shall comply with the latest edition of the references listed in each SEC directive, unless otherwise noted.

API 753	*Management of Hazards Associated With Location of Process Plant Portable Buildings*
ASTM A121	*Standard Specification for Metallic-Coated Carbon Steel Barbed Wire*
ASTM A123	*Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products*
ASTM A123M	*Zinc Coatings on Iron and Steel Products*
ASTM A529	*Standard Specification for Structural Steel With 42 000 Psi (290 Mpa) Minimum Yield Point ($^1/_2$ In. (12.7 Mm) Maximum Thickness*
ASTM A641	*Standard Specification for Zinc-Coated (Galvanized) Carbon Steel Wire*
ASTM A853	*Standard Specification for Steel Wire, Carbon, for General Use*
ASTM F1043	*Standard Specification for Strength and Protective Coatings on Steel Industrial Chain Link Fence Framework*
ASTM F1910	*Standard Specification for Long Barbed Tape Obstacles*
ASTM F1911	*Standard Practice for Installation of Barbed Tape*
ASTM F2453	*Standard Specification for Welded Wire Mesh Fence Fabric*
ASTM F2781 - 10	*Standard Practice for Testing Forced Entry, Ballistic and Low Impact Resistance of Security Fence Systems*
ASTM F567	*Standard Practice for Installation of Chain-Link Fence*
ASTM F626	*Standard Specification for Fence Fittings*
ASTM F668	*Standard Specification for Polyvinyl Chloride (PVC) and Other Organic Polymer-Coated Steel Chain-Link Fence Fabric*
ASTM F934	*Standard Specification for Standard Colors for Polymer-Coated Chain Link Fence Materials*
SEC-01	*General Requirements for Industrial Security*
SEC-03	*Security Gate*
SEC-04	*Security Lighting*
SEC-05	*Security Systems at Industrial Facilities.*
SEC-06	*Security Devices*
SEC-09	*Structures Housing Security Equipment*
SEC-13	*Industrial Facilities with Land-Water Interface*

5 General Requirements

5.1 Introduction

Facilities shall be protected by a fencing system in accordance with the requirements stated in this document.

5.1.1. The type of fencing system used in a facility shall be based on the FSC, as specified in SEC-01, which is approved by HCIS for the facility.

5.1.2. FO shall use one of the five distinct fencing system types designated Category 1 through Category 5. Category 1 provides the highest security while Category 5 is for lower security requirements.

5.1.3. Facilities consisting of multiple areas with different FSC's (such as a Process Area or an Administration Area) shall ensure that the area with the highest FSC shall have a contiguous fencing system consistent with the FSC of that area.

5.1.4. All fence penetrations (pipelines, conveyor systems, canals, power lines, etc.) shall meet the requirements of section 6.16 of this directive.

5.1.5. Facilities located in remote areas of the Kingdom or adjacent to open desert areas shall add additional surveillance measures to the perimeter layout to provide early warning and situational awareness, such as LRS cameras, thermal cameras, radar, or a combination of these technologies.

5.1.6. Facilities with a land-water interface perimeter shall require additional barrier measures on the land water interface as specified in SEC-13.

5.1.7. Existing roads located within 20m from the anti-personnel fence may be used as patrol roads under the conditions stated for each Category. The area between the existing road and the anti-personnel fence (clear zone) shall comply with the requirements of a clear zone to ensure a clear continuous view of the anti-personnel fence from the road.

Where existing roads are used as a patrol road, the clear zone shall not be less than 15 m wide for roads without traffic containment barriers and 10m for roads with traffic containment barriers.

5.1.8. In areas where internal or external patrol roads cannot be constructed as specified in this directive due to existing infrastructure, FO shall install additional fixed cameras for surveillance of that section of the perimeter fence.

5.1.9. Where facilities include Class 1 or Class 2 areas contiguous to Class 3 - 4 areas then the external patrol road shall be contiguous around the entire Class 1 through 4 perimeter.

5.1.10. The entire perimeter fence area shall be graded and cleared of all vegetation and maintained in this state. It shall have a 2% slope, away from the facility, to ensure proper water drainage.

5.1.11. No structures, fire hydrants, manholes, or other features shall be installed or located within the clear zone of any of the fencing systems.

5.1.12. Field Distribution Cabinets (FDC's) required for security system installations shall be located inside the facility perimeter but outside any specified clear zones. FO shall increase clear zone size to accommodate FDC's if needed.

5.2 Fence Definition Methodology

The fencing is defined by layout and the components that are installed within the layout.

5.2.1 **Layout**

All category fences shall consist of the following three main areas where fencing system components shall be installed:

5.2.1.1 ***External Interface Area***
This is the area on the outside of the anti-personnel fence.

5.2.1.2 ***Anti-Personnel Fence Area***
The area where the anti-personnel fence is installed.

5.2.1.3 ***Internal Interface Area***
This is the area on the inside of the anti-personnel fence.

5.2.2 **Components**

The following discrete components shall be installed in a specific layout specified below to produce a specific Category of fencing system:

5.2.2.1 ***Patrol Road***
A patrol road shall be level, a minimum of 4.6m wide and paved (concrete or asphalt) to ensure road is passable under all weather conditions.

5.2.2.2 ***Anti-Personnel Fence***

A fence with specified characteristics and design to deter and delay an intruder from entering the facility. Anti-Personnel fences may be constructed of chain-link or rigid weld mesh fence fabric.

5.2.2.3 ***Anti-Vehicle Barrier (AVB)***

A certified anti-vehicle barrier reinforces the fencing to prevent a vehicle from breaching the facility perimeter. Barrier details and certification requirements are specified in SEC-06.

5.2.2.4 ***Sensors***

Sensors deployed to detect intrusion attempts. SEC-05 provides details on sensor requirements.

5.2.2.5 ***Surveillance***

Surveillance devices deployed to evaluate and/or detect intrusion attempts. SEC-05 provides details on surveillance requirements.

5.2.2.6 ***Lighting***

Lighting deployed to illuminate the perimeter. SEC-04 provides details on lighting requirements at the perimeter.

5.2.2.7 ***Clear Zone***

The clear zone is an area adjacent to the anti-personnel fence (inside or outside) cleared of vegetation & obstructions and maintained in this state. Vegetation within the clear zone should not exceed 152mm in height.

These discrete components are combined and installed in the three main layout areas to achieve specified functionality.

The requirements for each category fence are summarized in the following sections followed by specific fence material and installation requirements in the Design Detail Section.

نسخة من خطة أمن شركة الفيصل الوطنية

5.3 Category 1 Fencing System

Category 1 fencing systems are used at facilities where the highest level of security is required and with an FSC of Class 1

The Category 1 fencing system components are as follows:

5.3.1 **External Interface Area**

The external interface area shall contain the outer patrol road and a clear zone.

This clear zone shall be 6m wide as measured from the inside edge of the patrol road to the anti-personnel fence.

Where existing roads are used section 5.1.7 shall apply.

5.3.2 **Anti-Personnel Fence Area**

The anti-personnel fence is contiguous with the edge of the external interface. It shall consist of a 3m high fence configured with three rolls of concertina wire.

A roll of concertina wire shall be mounted on top of the fence with a second roll mounted on the front top and the third roll mounted on the external bottom of the fence.

The anti-personnel fence shall be tested, validated and certified to provide forced entry resistance as specified in section 6.4.

Additional information on the fence fabric for the anti-personnel fence are in the Design Details section of this directive.

5.3.3 **Internal Interface Area**

The internal interface area consists of required components installed in the internal clear zone.

The internal clear zone shall be 10m wide as measured from the inside edge of the inner patrol road to the anti-personnel fence.

The components listed below shall be installed in this internal clear zone. FO may choose the specific installation location as long as it is within this internal clear zone and complies with the requirements of this directive.

*5.3.3.1 **Anti-Vehicle Barrier (AVB)***

The AVB shall be installed adjacent to the inside of the Anti-Personnel Fence.

It shall be crash rated, certified and installed as specified in SEC-06.

The AVB shall be non-obscuring to allow security patrols and perimeter monitoring and assessment systems to have a clear field of view through the AVB and anti-personnel fence.

*5.3.3.2 **Surveillance Systems***

Fixed surveillance cameras, fully compliant with SEC-05, section 5.8, shall be installed and sited so they look along the fence line and can view the entire internal and external interface areas of the fencing system.

Cameras shall be installed on a pole whose foundation is physically separate from anti-personnel fence or AVB foundations. The foundation shall be adequately sized to ensure that the camera imagery is stable and there are no vibrations that may compromise the ability of video analytics systems to detect and annunciate an alarm.

Surveillance cameras shall localize an alarm within 150m of the alarm location. Camera lateral spacing shall comply with the requirements of SEC-05, sections 5.8.2 & 5.8.3.

Assessment cameras, fully compliant with SEC-05, section 5.8, shall be provided to allow security personnel to assess an intrusion alarm. These cameras shall utilize a PTZ mount.

*5.3.3.3 **Sensors***

IDAS compliant intrusion detection sensors, as specified in SEC-05, shall be installed. SEC-05 requires two discrete intrusion sensor technologies.

*5.3.3.4 **Lighting***

Perimeter Lighting, as specified in SEC-04, shall be installed behind the sensors. Lighting luminaires shall be aimed so that they do not impact surveillance systems.

5.3.3.5 ***Inner Patrol Road***

The inner patrol road shall be located at the edge of the 10m internal clear zone.

Where existing roads are used section 5.1.7 shall apply.

5.4 Category 2 Fencing System

Category 2 fencing systems are used at facilities where a high level of security is required and with an FSC of Class 2.

The Category 2 fencing system components are as follows:

5.4.1 **External Interface Area**

The external interface shall contain the outer patrol road and a clear zone.

This clear zone shall be 6m wide as measured from the inside edge of the patrol road to the anti-personnel fence.

Where existing roads are used section 5.1.7 shall apply.

5.4.2 **Anti-Personnel Fence Area**

The anti-personnel fence is contiguous with the edge of the external interface. It shall consist of a 3m high fence configured with three rolls of concertina wire.

A roll of concertina wire shall be mounted on top of the fence with a second roll mounted on the front top and the third roll mounted on the external bottom of the fence.

The anti-personnel fence shall be tested, validated and certified to provide forced entry resistance as specified in section 6.4.

Additional information on the fence fabric for the anti-personnel fence are in the Design Details section of this directive.

نسخة من صفحة شركة الدراه الوطنية

5.4.3 Internal Interface Area

The internal interface consists of designated components installed in the internal clear zone.

The internal clear zone shall be 10m wide as measured from the inside edge of the inner patrol road to the anti-personnel fence.

The components listed below shall be installed in this internal clear zone. FO may choose the specific installation location as long as it is within this internal clear zone and comply with the requirements of this directive.

5.4.3.1 Surveillance Systems

Fixed surveillance cameras, fully compliant with SEC-05, section 5.8, shall be installed and sited so they look along the fence line and can view the entire internal and external interface areas of the fencing system.

Cameras shall be installed on a pole whose foundation is physically separate from anti-personnel fence or AVB foundations. The foundation shall be adequately sized to ensure that the camera imagery is stable and there is no vibrations that may compromise the ability of video analytics systems to detect and annunciate an alarm.

Surveillance cameras shall localize an alarm within 150m of the alarm location. Camera lateral spacing shall comply with the requirements of SEC-05, sections 5.8.2 & 5.8.3.

Assessment cameras, fully compliant with SEC-05, section 5.8, shall be provided to allow security personnel to assess an intrusion alarm. These cameras shall utilize a PTZ mount.

5.4.3.2 Sensors

IDAS compliant intrusion detection sensors, as specified in SEC-05, shall be installed. SEC-05 requires two discrete intrusion sensor technologies.

5.4.3.3 Lighting

Perimeter Lighting, as specified in SEC-04, shall be installed behind the sensors. Lighting luminaires shall be aimed so that they do not impact surveillance systems.

5.4.3.4 ***Inner Patrol Road***

The inner patrol road shall be located at the edge of the 10m internal clear zone.

Where existing roads are used section 5.1.7 shall apply

5.5 Category 3 Fencing System

Category 3 fencing systems are used at facilities where a medium level of security is required and with an FSC of Class 3.

The Category 3 fencing system components are as follows:

5.5.1 **External Interface Area**

The external interface zone contains a 6m wide clear zone as measured from the outside of the anti-personnel fence.

5.5.2 **Anti-Personnel Fence Area**

The anti-personnel fence is contiguous with the edge of the external interface zone. It shall consist of a 3m high fence configured with two rolls of concertina wire.

A roll of concertina wire shall be mounted on top of the fence with the second roll mounted on the front top.

The fence fabric shall either be chain-link or rigid weld mesh.

Additional information on the fence fabric for the anti-personnel fence are in the Design Details section of this directive.

5.5.3 **Internal Interface Area**

The internal interface zone consists of required components installed in the internal clear zone.

The internal clear zone shall be 6m wide as measured from the inside of the anti-personnel fence.

The components listed below shall be installed in this internal clear zone. FO may choose the specific installation location as long as it is within this internal clear zone and comply with the requirements of this directive.

نسخة مرخصة لشركة الميل الوطنية

5.5.3.1 ***Surveillance Systems***

Fixed surveillance cameras, fully compliant with SEC-05, section 5.8, shall be installed and sited so they look along the fence line and can view the entire internal and external interface areas of the fencing system.

Cameras shall be installed on a pole whose foundation is physically separate from anti-personnel fence or AVB foundations. The foundation shall be adequately sized to ensure that the camera imagery is stable and there is no vibrations that may compromise the ability of video analytics systems to detect and annunciate an alarm.

The imagery from these cameras shall be evaluated by a video analytics system that shall automatically annunciate an alarm in the SCC when an intrusion is detected.

PTZ mounted assessment cameras, fully compliant with SEC-05, section 5.8, may be located within the internal clear zone or may be located elsewhere within the facility as long as they have adequate zoom capability.

5.5.3.2 ***Lighting***

Area Lighting, as specified in SEC-04, shall be installed within the internal clear zone. Lighting luminaires shall be selected so that they do not impact surveillance systems.

5.6 Category 4 Fencing System

Category 4 fencing systems are used at facilities with an FSC of Class 4.

The Category 4 fencing system components are as follows:

5.6.1 **External Interface Area**

The external interface zone consists of a 6m wide clear zone as measured from the outside of the anti-personnel fence.

5.6.2 **Anti-Personnel Fence Area**

The anti-personnel fence is contiguous with the edge of the external interface zone. It shall consist of a 3m high fence configured with one roll of concertina wire mounted on top of the fence.

The fence fabric shall either be chain-link or rigid weld mesh.

Additional information on the fence fabric for the anti-personnel fence are in the Design Details section of this directive.

5.6.3 **Internal Interface Area**

The internal clear zone shall be 6m wide as measured from the inside of the anti-personnel fence.

The perimeter shall be illuminated with Area Lighting fully compliant with SEC-04. The lighting shall be located within this clear zone.

5.6.3.1 ***Surveillance Systems***

The entire perimeter of the facility shall be covered with CCTV surveillance & assessment cameras, fully compliant with SEC-05, section 5.7 & 5.8. The application of the cameras shall be determined by the SRA.

5.6.3.2 ***Lighting***

Area Lighting, as specified in SEC-04, shall be installed within the internal clear zone. Lighting luminaires shall be selected so that they do not impact surveillance systems.

5.7 Category 5 Fencing System

Category 5 fencing systems are used at facilities classified as Class 5 facilities.

The physical security implementation strategy and fencing system design for a Class 5 facility is specified in SEC-01, Appendix B.

5.8 Shared Fencing between Adjacent Facilities

Adjacent facilities sharing a perimeter fence present a special case for fencing. The design and implementation of shared fencing is based on both the timeline for facility construction and the FSC of each facility sharing the fence.

نسخة مرخصة لشركة تقنية لبيانات الوطنية

FO shall note that each FO is responsible for maintaining the integrity of their facility perimeter and ensuring it complies with FSC requirements.

5.8.1 As a general rule the facility that is constructed first shall implement all the perimeter fence requirements for the facility as described in this Directive and required by its FSC.

5.8.2 Facilities built after the first facility is constructed shall implement a modified version of the requirements to accommodate the requirements for an anti-vehicle barrier, perimeter intrusion detection and lighting.

5.8.3 Where both facilities have an FSC of Class 1 the shared fence section shall not require the following:

- External patrol road
- Anti-vehicle barrier

This applies when both facility outermost perimeters are continuous up to the shared fence sections on both ends.

5.8.4 The facility with the highest security classification (existing or new) shall be responsible for the installation and maintenance of the anti-personnel fence and the fence mounted intrusion detection sensors.

5.8.5 Existing facilities, with a shared fence, which are upgrading their security systems shall follow the same principle as in section 5.8.4 above. The first facility that is being upgraded shall implement all perimeter fence requirements as required by its FSC within its own property. This includes upgrading or replacing the anti-personnel fence, installation of intrusion detection sensors, CCTV surveillance and security lighting as required.

5.8.6 Where an AVB is required due to FSC requirements, FO may install an integrated solution at the anti-personnel fence. An integrated solution shall comply with SEC-06 requirements.

5.8.7 The external patrol road along the shared fence of Class 1 & 2 facilities is not applicable. Where the property along the shared fence is vacant land a temporary external patrol road shall be implemented.

5.8.8 Lighting shall comply with the requirements stated in SEC-04 for Shared Fence Lighting. Camera and sensor locations for each category fence shall be installed so that they minimize interaction between adjacent security systems.

5.8.9 The internal interface area for new and existing facilities shall contain all required components as specified under the specific fence categories in section 5.3 to 5.5.

5.8.10 Each facility shall construct and maintain an internal patrol road as specified in sections 5.3.3.5 and 5.4.3.4 above.

These requirements shall apply to facilities classified as Class 1, 2 or 3.

5.9 Internal Separation Fence

An administrative internal separation fence is utilized when a facility has a need to separate sections of the facility or specific assets in the facility such as a sub-station, dangerous chemical storage area, etc. from the rest of the facility. This fence shall be configured as a Class 4 anti-personnel fence. It shall not impact or be joined to the perimeter fencing systems used around the facility. The integrity of the perimeter fencing systems (intrusion detection, CCTV surveillance and patrol road) shall be maintained at all times.

Access gates shall meet the requirements as determined during the SRA and operational requirements.

In Class 1, 2 & 3 facilities where the administration areas and process areas utilize a single perimeter, an internal administrative separation fence shall be utilized. The separation fence for a Class 1 & 2 facility process area shall include a dedicated surveillance layer as described in sections 5.3.3.2 & 5.4.3.1 and all other requirements as specified for a Class 3 fence in section 5.5.

Access into the Class 1 & 2 process/operations area shall be via a SEC-03 compliant gate as specified in SEC-03 section 6.0 for a Class 3 facility.

5.10 Construction Fence

Construction fences are utilized to isolate a construction area or a construction site. This fence shall be configured as a category 4 anti-personnel fence.

During construction, the FO shall ensure that ongoing construction sites are isolated from existing facilities and process areas and adequate separation maintained from existing facilities.

Sections of the construction fence that are adjacent to a process area shall have all required perimeter protection systems operational as specified by the operational area FSC to maintain the perimeter integrity of the facility. This includes SEC-05 specified intrusion and surveillance systems.

5.11 Outer Property Fence

Outer property fences[1] are administrative fences used to define a property line that is remote from active process/operation areas of facilities with an FSC of Class 1, 2 or 3. This fence shall be configured as a Class 4 anti-personnel fence with an inner patrol road. This road may either be hard pack or asphalted at FO's discretion.

5.12 Clearances

5.12.1 **General**

All facilities shall ensure that critical elements and buildings intended for regular office occupancy are located at a distance from the perimeter anti-personnel fence as indicated below:

Class 1:	45m	*Critical elements only*
Class 2:	45m	*Critical elements only*
Class 3:	25m	*Critical elements only*
Class 4:	10m	*Critical elements only*

The FO shall identify the critical elements and buildings intended for occupancy in the facility and ensure their location complies with the clearance requirements. Typically, critical elements are items such as, but not limited to, main electrical facilities, non-water storage tanks, pump stations, control rooms and processing facilities. Buildings intended for occupancy are defined in API 753 Management of Hazards Associated with Location of Process Plant Permanent Buildings.

All buildings intended for occupancy shall be located to maintain a minimum clearance distance of 45m from the perimeter fence and any entrance gate.

These clearances apply to the distance that critical elements and occupied buildings are located from the anti-personnel fence and the AVB located at the gate. This does not apply to non-critical elements which can be located closer to the fence as long as fencing system requirements and safety and building codes are complied with.

[1] *Large mining concession areas shall not require an outer property fence*

Buildings intended for occupancy which cannot be located outside the 45m clearance zone shall be designed and protected as described in SEC-09.

5.12.2 **Coastal Facility**

Coastal facility clearance refers to the minimum distance, in front of the anti-personnel fence, to the high water mark.

If a facility is located in coastal areas the required clearance distance shall be 60m which will include the outer patrol road clearances.

This requirement does not apply to sea water intakes, port or fuel off-loading facilities, etc. with a land-water interface. The security requirements for these types of facilities are described in SEC-13.

5.12.3 **Gates**

All access gates into the facility shall be configured as specified in SEC-03 “Security Gate”. This includes main gates, internal gates, emergency gates and heavy equipment gates.

6 Design Requirements

All anti-personnel fencing and anti-vehicle barrier for a Class 1 facility requires detail designing to meet the requirements of this directive and the local soil conditions to maintain structural integrity at the specific location of installation.

The general design specifications and requirements for anti-personnel fencing are provided below.

6.1 Anti-Vehicle Barrier

The design and installation of the anti-vehicle barrier shall follow SEC-06 requirements.

6.2 Structural Performance

FO shall consider the local soil conditions and the maximum possible wind loads (highest wind speeds encountered in the area over the last 20 years) during the design phase of the fencing system to ensure and maintain fence structural integrity.

FO shall provide evidence that the results were incorporated into the design and installation of the anti-personnel fence and the AVB.

6.3 Durability Performance

Fence panels, and associated components, shall be galvanized in accordance with ASTM A641 requirements then fusion bond/polyester coated in accordance to ASTM F668. Galvanizing shall be applied after welding.

Terminal posts, corner posts, line posts, support braces, brace post, top rail, truss rods to be internally and externally galvanized in accordance to ASTM F1043 and then fusion bond/polyester coated internally and externally in accordance to ASTM F668.

A minimum coating thickness of 350micron shall be applied.

The color of the PVC shall be dark green or black as per ASTM F934.

Coatings damaged in the field during installation or operations shall be repaired using methods and techniques recommended by the manufacturer.

For RWM panels, after manufacture the entire panel shall be zinc-coated by a hot-dip galvanizing process to cover all weld locations, conforming to ASTM A123/A123M.

6.4 Forced Entry Resistance Performance

The anti-personnel fence shall be anti-cut/anti-climb and tested in accordance to ASTM 2781-10 with the following forced entry resistance times for Category 1 & 2 facilities:

- Medium threat level: 10 minutes
- Aggressive threat level: 5 minutes

These requirements shall be validated by a test report from an independent credible facility authorized to carry out such testing to ASTM F2781-10, or equivalent, standard. This report shall be submitted to HCIS for review and approval.

6.5 Fence Fabric & Panels

Anti-personnel fences may be constructed of either Chain-Link (CL) fabric or Rigid Welded Mesh (RWM) panels. In all cases, the fence must meet the Forced Entry Resistance Performance specified in section 6.4.

6.5.1 **Chain-Link Fabric**

Fabric shall be vinyl-coated[2] chain link with a typical 50 mm diamond mesh. The standard length of roll shall be 15m, or greater, and shall be woven continuously without splices.

6.5.2 **Rigid Weld Mesh Panel**

Rigid Weld Mesh panel widths shall be between 3m & 3.5m.

CATEGORY 1 & 2 FENCING SYSTEM: The fence shall have an aperture of 75mm x 12.5mm±2% center to center. Vertical reinforcing bars, 15mm wide x 5mm thick±2%, shall be placed at 75mm±2% intervals. The fence panel shall be constructed of vinyl-coated[2] machine welded mesh using 3mm±2% diameter wire unless otherwise specified.

CATEGORY 3 & 4 FENCING SYSTEMS: The fence shall have an aperture of 75mm x 12.5mm±2% center to center. The fence panel shall be constructed of vinyl-coated[2] machine welded mesh using 3mm±2% diameter wire unless otherwise specified.

6.6 Visibility Index (VI)

The Visibility Index (VI) specifies how security personnel patrolling the perimeter will have their view obscured by the fence fabric. It is computed by determining how much of the fence material in a single typical 3m panel obscures vision as listed below:

6.6.1 Determine total area covered by the width of all vertical and horizontal wires/strips in a single typical 3m panel (*not including razor tape or fence posts*) when viewed perpendicular to the fence line.

[2] *Exception: Galvanized fabric shall be permitted when required by section 6.10 or when needed for fence sensor performance*

6.6.2 Add coating thickness of all wires in the panel.

6.6.3 Determine the total surface area of the typical 3m panel (including all wires).

6.6.4 Subtract the area from 1 & 2 from the area calculated in 3.

6.6.5 Determine the % that is obscured.

This is the Visibility Index. The VI may not exceed 45%. This requires that no more than 45% of the fence panel area may be covered with fence wiring and strips.

6.7 Razor Tape

Razor Tape (i.e. concertina) materials and configurations shall be in accordance with ASTM F1910 with the following specific provisions:

6.7.1 Razor tape shall typically be 600 mm diameter (± 50 mm). Each loop shall consist of 24(±1) clusters of four needle-sharp barbs on 100mm centers, each barb measuring a minimum of 30mm in length.

6.7.2 The razor tape shall be secured along its entire length by a minimum 2mm thick rail with spikes on it.

Where required, razor tape shall be attached to the fence panel with a minimum 2mm thick bracket at 500mm intervals.

6.7.3 Where razor tape is placed on the ground, each coil shall be securely anchored to the ground at 1.5 meter intervals.

6.7.4 The fence posts shall be extended as needed to secure the razor tape.

6.8 Barbed Wire

6.8.1 Barbed wire shall consist of two strands of 12.5-gage galvanized wire according to ASTM A121, with 14-gage, 4-point barbs spaced 125mm.

6.8.2 Barbed wire shall be secured to the extension arm by lock wire. Lock wire shall be ASTM A641, 360mm long by 3.75mm nominal diameter wire, minimum, annealed and galvanized with a 25mm diameter hook on one end.

نسخة مرخصة لشركة المياه الوطنية

6.9 Tie Wire

6.9.1 Tie wire shall comply with the requirements for high-security round wire ties specified in ASTM F626.

6.9.2 FO may select any of the high-security tie wire methods specified in ASTM F626.

6.10 Concrete

Concrete used for fencing system installation shall comply with the following requirements:

6.10.1 The concrete mix formulation shall consider local soil type and potential impact from the water table.

6.10.2 Concrete shall have a minimum 28-day compressive strength of 28 MPa (4000 psi).

6.10.3 Cement shall be type V sulfate resistant.

6.10.4 Before placing components such as CL fabric, rails, tension wire & gates or RWM panels, the concrete shall have cured a minimum of 7 days unless the concrete reaches at least 75 percent of its design strength.

6.11 Grounding

6.11.1 Fences which are within 10m of an enclosed ground grid or ground loop that is connected to equipment operated at 1000V or greater shall not be PVC coated and shall be grounded at intervals not exceeding 15m to the ground grid or loop. All fences within 3 meters of a ground grid or ground electrode shall be bonded at the nearest fence post to the ground grid or ground electrode.

6.11.2 Fences that pass under a transmission line operating at 69kV and above shall not be PVC coated and be grounded at intervals not exceeding 15m on that portion of the fence within 100m of the power line.

نسخة من رخصة لشركة المياه الوطنية

6.11.3 Fences that cross over a ground grid or conductors that connect two ground grids shall not be PVC coated and shall have a bond[3] between the grid or conductors and the nearest post. If the crossing area is extensive, the bond is required every 50m.

6.12 Alignment & Terrain Profiling

6.12.1 Fence shall run in straight lines as far as possible. Where changes of direction are required the angle shall not be less than 90 degrees.

6.12.2 Fences shall match the terrain profile. When required due to terrain the fence panel width may be reduced from the nominal 3m width requirement and shorter panel widths be used with fence posts increased in length as needed. This may create a stepped profile on top of the fence. The razor tape shall seamlessly cover this profile.

6.12.3 Where the fence crosses features such as streams and drainage ditches and where conforming of the fence to the ground contour is impractical, the fence shall span the depression.

The space below the bottom of the fence shall be closed with extra fence panel or barbed wire. If extra length fence posts are required at such locations, they shall be furnished and installed in lieu of standard length posts as may be required.

6.12.4 A reasonably smooth profile at the fence line shall be provided. The bottom of the fence shall not be more than 25mm (1inch) above the finished ground line.

[3] *Exception: If the ground conductors used to connect the ground grids are insulated and sleeved with PVC conduit at points within 10m of the fence, then the bond is not required.*

6.13 Post Installation Requirements

6.13.1 All line posts shall be equally spaced at 3m intervals or less. Where RWM panels are used, post installation intervals shall match RWM panel size up to a maximum spacing of 3.5m.

6.13.2 Posts shall typically be 3.6m in length or as required by fencing system design**.**

6.13.3 Fence line, corner, end, gate, brace or pull posts shall be spaced as needed to guarantee fence stability or as required due to changes in vertical or horizontal alignment.

6.13.4 Posts to be coated both externally and internally.

6.13.5 The top of the installed post shall be covered with a cap that is secured using either a pop rivet, screw or bolt.

6.14 Chain Link Specific Requirements

The fence shall be installed in accordance with ASTM F567 and the specific provisions in this section.

6.14.1 **Fabric**

- The fencing fabric shall be attached to all line posts by means of tie wire.
- The chain link fence fabric shall be installed so that the posts are enclosed.
- The bottom of the chain link fabric shall be tied to a continuous concrete anchor[4].
- Tension bars shall be used with fabric bands.
- The bottom edge of fabric shall be fastened to the tension wire with wire ties.
- The fabric shall be stretched tautly so as not to deflect more than 76mm (3 inch) in the center of the fence panel in between the two line posts. Fabric shall be fastened securely to the posts.

[4] *Outer property fences, construction fences and internal separation fences do not require a continuous concrete anchor*

6.14.2 **Top Rail & Tension Wire**

- Fence shall be installed with a top rail and bottom tension wire.
- The top rail shall be continuous except over drive gates. One expansion/contraction coupling shall be used for every 30m of rail.
- If it is necessary for a top rail to be omitted, a top tension wire shall be installed.
- The tension wire shall be secured to the chain link fabric with high-security round tie wire.
- Tension wire shall be secured to terminal posts by means of a winding bracket.

6.14.3 **Bracing in Plane of Fence**

- Gate and end posts shall be braced to the nearest line post with one complete brace assembly.
- Corner and pull posts shall be braced to the two nearest line posts with one complete brace assembly to each line post.

6.14.4 **Barbed Wire**

- Six strands of barbed wire shall be installed to secure the razor tape installed on top of the fence.
- Strands shall be spaced uniformly and attached to frame with bands, clips, or eyebolts.
- The strands of barbed wire shall be stretched to remove sag and be anchored firmly to extension arms.

نسخة مرخصة لشركة الهيدال الوطنية

6.15 Rigid Welded Mesh Specific Requirements

Materials shall be uniform and consistent, conform to ASTM F2453 and shall meet the following requirements:

The fence shall be installed in accordance with *ASTM F567* and the specific provisions in this section.

6.15.1 **Fencing Panels**

- Panels shall be secured using bolts (min 5mm or 6mm thick), nuts and washers for fixing to be anti-tamper and made from Grade 316 or 304 Stainless Steel or hot dip galvanized.
- The fencing panels shall be attached to the line posts at intervals not exceeding 200mm along each post with locking plates, bolts, nuts and washers.
- Full locking system shall be positioned away from attack on the internal side of fence line.
- Bolts and nuts shall be tamper proof.
- The welded mesh fence panel shall be installed so that the posts are enclosed.
- If any damage occurs to the fence post or panels during installation, corrosion protection touch up should be applied within 48 hours.
- The bottom of the welded mesh panel shall be tied to a continuous concrete anchor[5] and fastened with wire ties at intervals not exceeding 250mm.

[5] *Outer property fences, construction fences and internal separation fences do not require a continuous concrete anchor*

6.15.2 **Barbed Wire**

- Six strands of barbed wire shall be installed to secure the razor tape installed on top of the fence.
- Strands shall be spaced uniformly and attached to frame with bands, clips, or eyebolts.
- The strands of barbed wire shall be stretched to remove sag and be anchored firmly to "Y" Shape extension arms.

6.15.3 **Miscellaneous Installation**

- Posts shall be one piece free of welded sections.
- Installation of razor tape shall follow the practice of ASTM F1911.

6.16 Fence Penetration

Pipelines, conveyer systems, culverts, storm drains, sewers, air intakes, exhaust tunnels, and utility openings that penetrate perimeter fencing shall comply with the following requirements:

6.16.1 **Penetration Type**

FO may use any of the following fence penetration methods:

- Under the fence
- Over the fence
- Through the fence

6.16.2 **General Requirements**

Any fence penetration design shall explicitly address the following concerns:

- No structures related to the fence penetration shall be constructed in the fencing system's internal interface or external interface zones.
- The penetration shall have specific measures to prevent an intruder from utilizing the fence penetration as a route to enter the facility. The prevention measures shall vary based on the penetration type.
- Additional surveillance cameras shall be installed at the fence penetration point. These cameras shall be dedicated to monitoring the fence penetration point.
- The video from these cameras shall be analyzed by a video analytics system at the SCC for automatic alarm annunciation.

نسخة مرخصة لشركة لمداد الوطنية

- The functioning and layout of the perimeter security system shall not be impacted by the penetration.
- Stout guardrails shall be installed at the transition point where the pipeline enters/exits the ground to prevent vehicle damage to the pipeline.

6.16.3 **Under Fence Penetration**

- Under fence penetrations shall be limited to pipelines. Conveyor belts shall not utilize an under fence penetration.
- Pipelines shall be buried outside the perimeter fencing system external interface and internal interface zones.
- The pipeline may either be directly buried or use a culvert depending on operational requirements
- If the under fence penetration requires the construction of a concrete culvert then it shall comply with the following:
  - The opening shall be sealed on both sides with bars and a collar to prevent ingress of humans or small animals.
  - The bars/grates shall have sensors installed to detect tamper/breach attempts.
  - The bars and collar and fence shall conform to the culvert shape. Steel used for the grill must be in accordance with ASTM A529 and ASTM A123 for corrosion prevention.

6.16.4 **Over Fence Penetration (Pipelines & Conveyer Systems)**

- Over fence penetrations shall be at an adequate height so that they cannot be used to facilitate entry into the facility and will not impact the functioning and layout of the security system.
- All exposed pipes shall be retained at constant height above the fencing system internal and external interface zones.
- For Class 1, 2 & 3 fencing systems the pipeline on exterior side of fence, and 5m on the inside of the fence, shall be covered with concertina wire, installed the same way as the top of a Class 1 fence. The concertina shall terminate 2.5m before ground entry on the exterior side of the fence or 20m from the anti-personnel fence.
- For Class 4 fencing systems pipeline on both the interior, and exterior, side of the fence shall be covered with concertina wire for a distance of 5m centered on the fence.

6.16.5 **Through Fence Penetration**

- The fence height shall be increased to maintain 3m fence height over the top of the penetration.
- Anti-personnel measures shall be deployed for the distance of the external clear zone to prevent intruders approaching the fence line.
- The area under and around the penetration shall be sealed against intruders.

6.16.6 **Conveyer Systems with Cat-Walks**

- A conveyer system shall be closed off at the point of penetration with anti-personnel measures to prevent any human crossing along the conveyer.
- Dedicated fixed CCTV cameras, equip with video analytics, shall cover the top and bottom areas of the conveyer system.
- Gates on the cat-walks to allow for maintenance shall be fitted with an alarm system to ensure closure of the gates at all times.
- Conveyer system support pillars external to the facility shall be protected with anti-climbing measures.

6.17 Emergency Gates

6.17.1 Emergency gates shall be designed in accordance with applicable SEC-03 section 5.20.5 requirements.

6.17.2 Emergency gates shall have dedicated video surveillance that is monitored in the local SCC.

6.17.3 Emergency gate width shall be at least 5m to allow the movement of emergency vehicles.

6.17.4 Emergency gates shall have the same anti-personnel characteristics, sensors and surveillance as facility perimeter fencing based on the facility FSC.

6.17.5 Chain link gates for a Class 1 & 2 facility shall not be acceptable.

7 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on its FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Class 1 Fencing	✓				
Class 2 Fencing		✓			
Class 3 Fencing			✓		
Class 4 Fencing				✓	
Shared Fencing between Adjacent Facilities	✓	✓	✓		
Outer Property Fence	✓	✓	✓		
Clearances - General	✓	✓	✓		
Main Gates	✓	✓	✓	✓	
Emergency Gates	✓	✓	✓	✓	
Design Requirements for Fencing System Components	✓	✓	✓	✓	
Installation	✓	✓	✓	✓	
Fence Penetration	✓	✓	✓		

نسخة خاصة لشركة المياه الوطنية

8 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items. The Stage 3 submission, content and format are specified in SEC-14 section 6.3. This PoC shall form part of Section 3 of the Stage 3 submission package.

This PoC shall provide technical details for each of the requirements listed below.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-02 Reference	Requirement	FO Response
1.	5.3 – 5.6	Category 1- 4 fencing system	*Provide design drawings, with dimensions, for ALL applicable category fencing system layouts as defined by the FSC*
2.	5.8	Shared Fence	*Provide design drawings, with dimensions, for ALL applicable shared fencing system layouts.*
3.	5.9	Internal Separation Fence	*Provide design drawings, with dimensions, for ALL applicable internal separation fence layouts that separate administrative areas from operational areas.*
4.	5.10 – 5.11	Construction & outer property fence	*Where applicable:* *Provide design drawings, with dimensions, for ALL construction fences and the outer property fencing*
5.	5.12	Clearances	*Provide layout map indicating clearances to critical element*
6.	6.2	Structural Performance	*Provide structural design basis*
7.	6.16	Fence Penetrations	*Where applicable:* *Provide design drawings, with dimensions, for ALL fence penetrations*

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-03

Security Gates

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7
2 SCOPE 7
3 ACRONYMS & DEFINITIONS 7
4 REFERENCES 8
5 GENERAL REQUIREMENTS 9
5.1. Gate Design 9
5.2. Preliminary Inspection Checkpoint 10
5.3. Vehicle Approach Speed Management 11
5.4. Auxiliary Gate 12
5.5. Gatehouse 13
5.6. Traffic Management 15
5.7. Additional Inspection Area 16
5.8. Over Watch 16
5.9. Pedestrian Access 17
5.10. Gate Support Buildings 17
5.10.2. X-Ray & Inspection Building 18
5.10.3. Visitor Center 19
5.11. Communications 19
5.12. Lighting 20
5.13. Environmental 20
5.14. Access Management 20
5.15. Surveillance Cameras 21
5.16. Response Zone 21
5.17. Gate Clearances 22
5.18. Power Systems 22
5.19. Unmanned Gates 23
5.20. Gate Types 23
6 APPLICATION OF REQUIREMENTS 25
7 PROOF OF COMPLIANCE 26
8 SAMPLE DRAWINGS 27

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This Security (SEC) directive provides requirements for the design of facility security gates.

2 Scope

This standard provides Facility Operators (FO) with the general requirements for security gates at facilities under the jurisdiction of the HCIS.

3 Acronyms & Definitions

AVB	Anti-Vehicle Barrier: There are three types of AVB: • Deployable AVB: *This type of AVB is deployed at gates in the vehicle traffic lanes & is commonly referred to as a* Road Blocker. • Fixed AVB: *This type of AVB is deployed as part of the perimeter fencing system.* • Bollards: *Bollards may be fixed or deployable. They are required for traffic management and roadway containment in the gate area.*
CMU	Concrete Masonry Unit
FO	Facility Operator: Owner, operator or lessee of a facility
FSC	Facility Security Classification
HCIS	High Commission for Industrial Security
LAN	Local Area Network
PIC	Preliminary Inspection Checkpoint
PTZ	Pan/Tilt/Zoom
SCC	Security Control Center
SEC	Security Directives
SECNET	Security Network
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
SOW	Scope of Work
SRA	Security Risk Assessment
VASM	Vehicle Approach Speed Management

نسخة من شبكة الاتصالات الوطنية

4 References

This directive adopts the latest edition of the references listed.

API 780	*American Petroleum Institute (API)* *API Recommended Practice 780* *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*
ASTM 2656-07	*American Society for Testing and Materials (ASTM)* *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*
CCPS	*Center for Chemical Process Safety (CCPS)* *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*
NIJ 0108.01	*National Institutes of Justice Standard 0108.01* *Ballistic Resistant Protective Materials*
SEC-01	*General Requirements for Security Directives*
SEC-02	*Security Fencing*
SEC-04	*Security Lighting*
SEC-05	*Security Systems at Industrial facilities*
SEC-06	*Security Devices*
SEC-07	*Power Supplies*
SEC-08	*Security Communications & Data Networks*
SEC-09	*Structures housing Security Equipment*

نسخة غير معتمدة من شركة المياه الوطنية

5 General Requirements

The gate architecture specified in this Security Directive specifies the minimum requirements for gates at industrial facilities.

The gate architecture is based on managing the approach to a facility, inspection at the gate, access management and containment of unauthorized intrusion attempts. Collectively these are referred to as the "security gate" and the layout comprises the gate architecture.

Full containment and control of all vehicles and personnel is required at all gates. This shall be achieved through a combination of active and passive barrier systems managed by on-site security personnel.

Each element of gate architecture is detailed in the following sections:

5.1. Gate Design

The specific gate architecture for each facility gate shall be determined during the SRA process which includes an analysis of the function and location of the gate and the FSC of the facility.

The design for each gate in a facility shall include three clearly defined zones or areas:

5.1.1. Approach Zone. This is the area external to the gate in which vehicles and pedestrians move towards the gate.

5.1.2. Access Control Zone. This is the area immediately in front of the gatehouse where vehicles and pedestrians are cleared and authorized to pass through the gate.

5.1.3. Response Zone. This is the area where the gate security personnel respond and take action to allow access or prevent access.

The gate architecture required for each class of facility is stipulated in section 6 of this directive.

5.2. Preliminary Inspection Checkpoint

The function of the PIC is to conduct a pre-screening/inspection of vehicles/personnel approaching a Class 1 or Class 2 facility and to ensure they are authorized to approach the facility. It provides early warning to gate personnel of potentially hazardous payloads. It is typically manned by government forces.

The PIC shall meet the following requirements:

5.2.1. It shall be located 100m – 300m before the facility gate. The PIC and PIC area shall be designed so that the PIC cannot be bypassed by any vehicle approaching the facility or the facility gate.

5.2.2. Traffic approaching the PIC, and all the way through the PIC, shall be channelized using medians, or other separation obstacle, to divide incoming and outgoing traffic. The median height shall be at least 152mm.

The median shall start at least 10m before the PIC.

5.2.3. The median shall be sized to provide a safe location for security personnel to stand and examine vehicles. It shall have bollards installed for security personnel protection.

5.2.4. The PIC shall have a protected shelter for PIC security personnel. PIC's deployed after the release of this directive shall comply with the ballistic requirements for the shelter as specified in section 5.5.4 below.

5.2.5. Checkpoint lighting, as specified in SEC-04, shall be installed.

5.2.6. The PIC shall be equipped with reliable communication to the local gatehouse and the SCC. It shall have an emergency button to manually annunciate an alarm at the local gatehouse and SCC.

5.2.7. Parking for at least 5 full sized vehicles, as generally encountered at the facility, shall be provided adjacent to the PIC. Additional parking shall be catered for if traffic estimates require it.

5.2.8. The PIC area shall be covered with a sunshade.

5.2.9. PIC design shall incorporate VASM to limit vehicle approach speeds. Each incoming vehicle lane shall deploy a raise arm barrier, as specified in SEC-06, for management of incoming traffic.

If the raise arm barrier boom is broken an alarm shall automatically be annunciated at the PIC and the gate house.

5.2.10. A security road spike barrier (tire shredder) shall be installed in the exit lanes at the PIC. This barrier shall comply with the following:

5.2.10.1. Cover at least 90% of each PIC exit lane width.

5.2.10.2. Laid out so that no vehicle may bypass the spikes

5.2.10.3. Spikes shall be rated for the maximum weight of any vehicles expected to traverse the exit lanes.
At a minimum the spikes shall be rated for a 20 ton vehicle weight.

5.2.10.4. Spikes shall be oriented so that any vehicle approaching the PIC exit lane from the wrong direction shall have their tires disabled.

5.2.10.5. Drainage shall be installed as needed to prevent water accumulation around the barrier.

5.2.10.6. The spike barrier shall be regularly maintained to ensure full functionality at all times.

5.3. Vehicle Approach Speed Management

5.3.1. The roadway approaching a gatehouse shall have a chicane or zigzag design to retard the speed of incoming vehicles. This may be augmented by additional speed retardation devices and designs if so required by the FO. A 90 degree (90°) turn leading to the gatehouse shall be an acceptable alternative to a chicane.

5.3.2. Where space for a chicane is not available the FO shall utilize other speed control devices to implement the intent of VASM.

5.3.3. The chicane shall be designed so that the maximum speed for a 6800kg truck through the VASM is limited to 40kph.

5.3.4. The approach to the gatehouse after the chicane / speed control devices shall be no longer than 50m in order to minimize the distance the vehicle has available to accelerate to the gatehouse.

5.3.5. The sides of the roadway in the chicane shall have barriers that shall prevent a vehicle from driving or cutting across the chicane.

5.3.6. The chicane shall be designed to allow long loads and articulated loads to pass safely through. Any design elements that facilitate the passage of such loads shall not compromise the intent of VASM.

5.3.7. VASM measures shall not obstruct the line-of-sight between the PIC and the gate.

5.4. Auxiliary Gate

5.4.1. The auxiliary gate shall provide the capability to shutdown pedestrian or vehicle lanes or the entire gate as needed.

5.4.2. When the auxiliary gate is deployed to close a lane or lanes, the AVB's in those lanes must be deployed.

5.4.3. It shall consist of a steel gate that can be used to close selected entry or exit lanes or to close all lanes when they are not needed.

5.4.4. Chain link gates shall not be acceptable.

5.4.5. The auxiliary gate shall be designed to prevent any person entering the facility when the gate is closed.

5.4.6. The FO shall ensure that anti-personnel measures are incorporated in the gate design to prevent an intruder from entering under, through or climbing over the gate when it is closed.

5.4.7. Gates shall be constructed of strong steel elements that present a reasonable degree of anti-vehicle protection.

5.4.8. The auxiliary gate shall be at least 3.0m high and shall be able to cover all lanes. Multiple segments shall be used for the gate if needed.

5.4.9. The auxiliary gate shall be located on the outside of the facility and within 3m - 10m of the gatehouse.

5.4.10. All gate segments shall have positive locking mechanisms to maintain gate integrity and security.

5.4.11. Locks used on this gate shall be fully compliant with SEC 09.

5.4.12. The gate shall use either a motorized sliding or swing mechanism for deployment.

نسخة من خط أنابيب الغاز الوطنية

5.4.13. Clearance between the bottom of the auxiliary gate and the road surface shall at no point be more then 50mm.

5.5. Gatehouse

The gatehouse shall house security personnel and security system components to manage access to the facility.

5.5.1. The gatehouse shall be sized to accommodate security personnel and equipment assigned to the gate. Gatehouse sizing shall be recommended by the SRA and approved by HCIS prior to construction.

5.5.2. The gatehouse windows shall comply with the requirements for ballistic-resistant glass specified in SEC-06.

5.5.3. Openings in the windows for document inspection are permitted as long as they do not compromise the ballistic protection levels.

5.5.4. The walls of the gatehouse shall provide ballistic protection to NIJ 0108.01, Level III.

The walls shall be constructed of reinforced concrete or grouted CMU. The thickness of reinforced concrete shall be not less than 165mm and grouted CMU walls not less than 205mm.

Alternative methods of construction, such as prefab panels, prefab gatehouses or polymer reinforcements, shall be acceptable as long as ballistic protection to NIJ 0108.01, level III is provided.

Any alternative method of construction shall have its protection level certified by independent internationally recognized authorities, as being fully compliant to Level III requirements of NIJ 0108.01.

5.5.5. The gatehouse shall have 360 degree visibility.

5.5.6. The gatehouse shall be installed on a base raise a minimum of 500mm above the roadway.

5.5.7. The side of the gatehouse facing the outside and inside shall be protected by a concrete barrier.

5.5.8. This barrier shall be located on the gatehouse base and consist of a raise circular barrier at least 70cm high across the full width of the gatehouse. It

shall be constructed of steel reinforced concrete anchored 300mm below grade to increase resistance to impact. The barrier height shall not impede visibility from the gatehouse. The barrier shall be located within 3m of the gatehouse building.

5.5.9. The entrance door to the interior of the gatehouse shall be on the side of the gatehouse facing towards the inside the facility. No entrance shall be on the front or sides of the gatehouse.

5.5.10. The exterior door of a gatehouse shall not restrict 360 degree visibility and comply with the requirements for exterior doors, door frames and the ballistic requirements as specified in SEC-06 & SEC-09.

5.5.11. Gatehouse interior lighting shall comply with the requirements of SEC-04.

5.5.12. The gatehouse shall have LAN connectivity that connects the gatehouse to SECNET and FO's network as needed.

5.5.13. All electrical switchgear for gatehouse devices shall be inside the facility perimeter close to the gatehouse.

5.5.14. Power to the gatehouse shall clearly distinguish between commercial power and UPS power by the use of distinct outlets for each power source. Power outlets sourced from UPS power shall only be used for designated security devices and no extra UPS outlets, other what are required, shall be installed.

5.5.15. Power to the gatehouse and all security devices shall comply with the requirements of SEC-07.

5.5.16. The installation of equipment, large screen TV monitors, workstations, furniture or documents shall not impede the view from inside the gatehouse.

5.5.17. The area above the gatehouse and inspection lanes shall be covered with a sunshade. The sunshade shall have adequate clearances to allow trucks and vehicles to enter the facility.

5.5.18. The sunshade shall extend to an adequate distance on both sides of the gate to cover positions where security personnel will conduct inspections. The sunshade extension to cover these positions shall allow for gate orientation and the suns position to optimize coverage at all times of day.

5.5.19. An audible and visual alarm shall be provided that shall be activated during an emergency.

The intensity of the audible alarm shall be audible to all personnel in the gate area. The visual alarm shall be placed in multiple locations if needed to ensure clear visibility to all personnel in the gate area.

Activation of the alarm shall be by a pushbutton in the gatehouse. The pushbutton shall be protected against accidental activation but shall not be locked at any time.

Activation of the alarm shall annunciate an alarm at the SCC that is monitoring the gate.

5.5.20. Only security devices that require security personnel interaction or view shall be installed in the gatehouse. The gatehouse may not be used for the installation of other security system support equipment.

5.5.21. While the gatehouse may be used to display alarms for specified security related activities at the gate, it may not be used for SCC functions, unless specifically identified and recommended in the SRA and approved by HCIS.

5.6. Traffic Management

5.6.1. Each lane in the gatehouse inspection area shall have medians separating each lane of traffic. The medians shall be sized to allow installation of equipment and permit a safe location for personnel to stand on. The height of the median shall be sized as needed for operational needs but shall be at least 152mm high.

5.6.2. The traffic management design shall incorporate a rejection lane where vehicles denied access shall be able to turn around without entering the facility. The rejection lane turning radius shall be sized for the largest vehicle expected to enter the facility. The rejection lane/turning point shall be located before the gatehouse.

5.6.3. There shall be adequate parking on the inside and outside of each gate to allow parking of gate personnel and visitors without obstructing traffic flow.

5.6.4. Each lane shall have a clearly visible traffic light type setup that will inform users from a distance if a lane is open or closed.

5.6.5. All lanes and traffic flow directions shall be clearly marked on the roadway.

5.6.6. Roadway containment in the access control & inspection area shall prevent inbound vehicles from unauthorized access and shall extend from the inspection area to the end of the Response Zone.

5.6.7. The containment shall consist of passive barriers on either side of the roadway that shall deny a vehicle entry to the facility until the end of the Response Zone. The passive barriers on either side of the roadway shall fully comply with the requirements of SEC-06.

5.6.8. The location of pedestrian access points (turnstiles) in the gate area shall consider the safety of pedestrians and prevent them from crossing into vehicle lanes.

5.7. Additional Inspection Area

5.7.1. The additional inspection area is a space where detailed inspections of vehicles & document inspection can be carried out without obstructing traffic flow.

5.7.2. There shall be adequate space before or adjacent to the gatehouse for gate security personnel to conduct additional vehicle inspections without obstructing traffic flow.

5.7.3. A shaded or enclosed location shall be provided in the additional inspection area where K-9 services may be located when needed by the local security requirements.

5.7.4. The additional inspection area shall be located as close as possible to the gatehouse.

5.7.5. This area shall always be within line-of-sight of gatehouse personnel.

5.8. Over Watch

The over watch position sets up a location where heavy, mounted weapons can be deployed to support gatehouse personnel. Manning of the over watch position shall be at the discretion of the FO, HCIS and Saudi Government security agencies assigned for facility protection.

5.8.1. The FO shall establish an over watch position, covered with a small sunshade that will allow mounted weapons to be deployed with the gatehouse in clear line of sight.

5.8.2. The over watch position shall be within 100m of the gatehouse and shall be located inside the facility perimeter.

5.8.3. Where possible, the over watch position shall be located at an elevated vantage point to provide an unobstructed field of fire to support gatehouse security personnel.

5.8.4. Over watch positions shall be required at all gates into facilities which are located in the external perimeter of the facility.

5.9. Pedestrian Access

The design of all gates shall provide for safe pedestrian access. All pedestrian access shall be controlled and recorded through electronic access control systems integrated with a turnstile as required in SEC-05 and SEC-06.

Pedestrian access points installed more than 50m from the gate area shall meet all the requirements for surveillance, check point lighting and screening of personnel and a gate support building as stipulated in section 5.10 below, SEC-04 & SEC-06.

Gates which are not intended for pedestrian use, and identified as such in the SRA, may omit the equipment required for pedestrian access control.

5.10. Gate Support Buildings

Gate Support buildings are used to house gate related equipment and facilities. They shall be located within the perimeter fence.

5.10.1. General Requirements

5.10.1.1. Gates with access control system, intrusion detection system or X-ray & Inspection equipment shall require a support building with toilet and prayer facilities and separate, dedicated rooms for security system support equipment installation.

5.10.1.2. Gates without access control system, intrusion detection system and X-ray & Inspection equipment deployments shall only require toilet and prayer facilities in a support building if the nearest existing toilet facilities are more than 20m away.

5.10.1.3. Network equipment shall be installed in a dedicated room in the gate support building. Network equipment shall not be installed in the gatehouse.

5.10.1.4. Gate support buildings shall be constructed of CMU with rebar and grout in every core of every block or reinforced concrete construction to provide ballistic protection to level III of NIJ 0108.01.

5.10.1.5. Entry doors and door locks shall be fully compliant with the requirements of SEC-09.

5.10.1.6. The environmental system shall comply with the requirements of SEC-01 and SEC-05 for housing security system components.

5.10.1.7. The Gate Support Building may incorporate the Visitor Center as described in section 5.9.3.

5.10.1.8. An audible and visual alarm as stipulated in section 5.5.19 shall be provided for all Gate Support Buildings occupied by security personnel.

5.10.1.9. All Gate Support Buildings shall be protected with an anti-vehicle barrier deployed on all sides facing traffic.

5.10.1.10. Gate support buildings occupied by security staff shall be within unobstructed line of sight to each other.

5.10.2. **X-Ray & Inspection Building**

5.10.2.1. All gates providing access into a Class 1, 2 or 3 area shall be equipped with an X-ray system and metal detection archways as stipulated in SEC-06 for the detection of contraband.

5.10.2.2. The X-ray system and metal detection archway shall be located in a building near the gate to provide easy access for pedestrians, drivers and passengers of vehicles to pass through the inspection area.

5.10.2.3. The x-ray & inspection building and equipment, location and layout shall be designed as to prevent pedestrians from bypassing x-rays & inspection.

5.10.2.4. The X-ray unit shall be co-located with a pedestrian access control system specified in SEC-05.

5.10.2.5. The X-ray Building shall comply with all the environmental requirements as stipulated in SEC-01.

5.10.2.6. The X-ray & Inspection Building shall provide ballistic protection to the security staff to level III of NIJ 0108.01.

5.10.2.7. All areas and activities inside the X-ray & Inspection Building shall be covered with area surveillance CCTV cameras monitored in the SCC.

5.10.2.8. Gates which are not intend for pedestrian use, and identified in the SRA as a "Truck Gate" with no risk of passengers entering the facility, may omit the "Search Facility" with X-ray system and Metal Detection Archways.

5.10.3. **Visitor Center**

5.10.3.1. The main entrance gate of Class 1, 2 & 3 facilities shall include a Visitor Center for the processing of visitors into the facility.

5.10.3.2. The Visitor Center may be integrated with the X-ray & Inspection Building.

5.10.3.3. The building shall provide ballistic protection to the security staff to level III of NIJ 0108.01.

5.10.3.4. The Entrance and Reception Area for visitors shall be covered with area surveillance CCTV cameras monitored in the SCC.

5.10.3.5. The gatehouse at a Class 4 facility may also be used for visitor registration.

5.11. <u>Communications</u>

5.11.1. Communication systems deployed at the gatehouse, X-ray & Inspection Building and Visitor Center shall comply with the requirements of SEC-08.

5.11.2. SEC-08 compliant hotlines and radios from all gate buildings occupied by security staff shall be provided to the SCC.

5.11.3. Each Gatehouse & Gate Support Building shall have at least 2 dedicated telephone lines.

5.12. Lighting

5.12.1. The gate, and PIC area, shall have checkpoint lighting installed that is fully compliant with SEC-04.

5.12.2. The area along the roadway centered at the gatehouse and 100m on both the entry and exit side shall have area lighting installed that is fully compliant with SEC-04.

5.12.3. Interior lighting of all gate buildings shall comply with the requirements of SEC-04.

5.13. Environmental

5.13.1. All enclosed structures deployed for compliance with the requirements of this Security Directive shall have air conditioning that is fully compliant with SEC-01.

5.13.2. All equipment deployed for compliance with the requirements of the Security Directives shall be certified for extended, continuous operation under the environmental conditions stated in SEC-01.

5.13.3. The gatehouse and gate support buildings shall be air conditioned to meet the environmental requirements specified in SEC-01.

5.14. Access Management

5.14.1. Gates leading into industrial facilities shall deploy access control systems as specified in SEC-05.

5.14.2. All access management devices deployed for implementing Security Directives shall meet the requirements of SEC-05 and SEC-06.

5.14.3. The area around the gate and around the entire perimeter shall be fenced so that employees and visitors cannot enter the facility without being cleared by gate security personnel.

5.14.4. FO shall install/deploy access control devices (such as raise arm barriers) in each traffic lane in the access control zone of the gatehouse to prevent vehicles entering the gatehouse area without clearance.

5.14.5. FO shall install turnstiles fully compliant with the requirements of SEC-06 as an access control measure at all pedestrian entry/exit points.

5.14.6. FO shall implement an X-ray examination system using X-ray units fully compliant with the requirements of SEC-06. This X-ray system shall be used to examine all packages entering the facility.

5.14.7. No personal vehicles shall be permitted in restricted areas.

5.14.8. FO shall develop documented access control & inspection procedures for all vehicles, pedestrians and material; and applied to each lane of the gate and all pedestrian entry/exit points.

All access points into a facility shall keep track of all personnel & vehicles entering the facility.

Security personnel shall execute this procedure at the gatehouse after receiving adequate training as specified in SEC-01. The procedures shall be available in the gatehouse for inspection by HCIS.

5.15. Surveillance Cameras

5.15.1. FO shall use fixed cameras for surveillance and PTZ cameras for assessment in the gate area.

5.15.2. Surveillance shall include the surrounding area of all gate buildings, approach to each building and all traffic and pedestrian lanes. A minimum of one PTZ camera shall be installed on the entry side of the gate and one PTZ camera for the exit side of the gate.

5.15.3. These cameras shall have an adequate field of view and focal length to view both sides of the gate and the gatehouse. They shall have a clear view of pedestrian and vehicle traffic entering and exiting the facility.

5.15.4. All vehicle traffic lanes in the gate area and all pedestrian entry/exit point shall have a dedicated fixed camera for surveillance and identification of vehicles, including the top of heavy vehicles.

5.15.5. Cameras shall be monitored in the SCC monitoring the facility.

5.15.6. SCC personnel shall be provided with a full set of controls to manage and view the PTZ camera imagery.

5.15.7. All cameras shall be VASS compliant.

5.16. Response Zone

5.16.1. The response zone is the area from the gatehouse and beyond where security personnel can activate a deployable AVB which shall prevent unauthorized vehicles from entering the facility after passing through the access control & inspection area.

5.16.2. The AVB shall be a certified anti-vehicle AVB fully compliant with the requirements of SEC-06.

5.16.3. The length of the response zone shall be calculated based on the configuration of the gate and calculated from the rear end of the gatehouse.

A shorter response zone length may be used if speed control measures are put in place that limits initial vehicle velocity at the gate.

5.16.4. AVBs shall be located in both entry and exit lanes. AVB deployment shall be via gatehouse personnel or SCC personnel. Retraction of the AVB after emergency deployment shall require a key switch or an online command from the SCC. Keys shall be maintained and kept only in the SCC.

5.16.5. Gatehouse personnel shall have a clear view of the roadway between the gatehouse and the AVB to ensure routine AVB deployment will not cause problems when vehicles are traversing the roadway.

Active sensors shall be used to ensure that vehicles will not be affected by AVB deployment. These sensors shall be wired into the routine deployment switch but shall be ignored if an emergency deployment is activated.

5.16.6. Roadway containment shall be installed from the access control & inspection area up to the end of the Response Zone.

The containment shall consist of passive barriers on either side of the roadway that shall prevent a vehicle from taking any alternate route other than the roadway.

The passive barriers on either side of the roadway shall fully comply with the requirements of SEC-06.

5.16.7. AVB's shall not be installed next to or in line with the gatehouse.

5.16.8. AVB's shall not be co-located with a raise arm barrier. The minimum distance between the AVB and the raise arm barrier shall be calculated as described in 5.16.2 and sufficient to accommodate the largest vehicle expected to enter the facility.

5.17. Gate Clearances

Refers to the minimum distance, beyond the AVB that is deployed in the gate area (response zone), at which a critical asset or occupied building inside a facility may be located.

The clearance distances for Class 1, 2, 3 & 4 facilities are specified in SEC-02, section 5.12.1.

5.18. Power Systems

All power systems deployed to the gate and gate support facilities shall comply with the requirements of SEC-07.

5.19. Unmanned Gates

Class 1, 2 & 3 facility gates that are not manned 24/7 shall have surveillance cameras and intrusion sensors that are activated when the gate is unmanned. The cameras and sensors shall be monitored at the local SCC. The cameras and sensors shall provide the same level of monitoring as the rest of the perimeter.

5.20. Gate Types

5.20.1. Main Gate

The Main Gate is located in the facility perimeter and provides the main access for pedestrians, light vehicles or trucks, into an industrial facility. A Visitor Center is located at this gate to process visitors and personnel without access cards. This gate shall implement the gate architecture required for the FSC and SRA recommendations.

5.20.2. Process/Operations Area Gate

A Process/Operations Area Gate provides access into the facility process or operations area. Process/Operations Area Gates are high security gates and shall implement the full gate architecture required by the Process/Operations Area FSC and SRA recommendations.

5.20.3. Internal Gate

An Internal Gate is located in an internal separation fence as described in SEC-02, section 5.9. The gate architecture is determined by the SRA and operational requirements.

Internal gates inside process areas that administratively separate different process functions do not require a gatehouse.

5.20.4. Administrative Gate

Any gate, other than the Main Gate, that is located in the facility perimeter such as a Truck Gate, Maintenance Gate, etc. shall implement the gate architecture required for the FSC and SRA recommendations. Such a gate, when located in the perimeter of a Class 1 or Class 2 area, shall include all the requirements stipulated in this Directive.

5.20.5. Emergency Gate

Emergency Gates are located in the facility perimeter to allow emergency vehicles into the facility or the evacuation of personnel during an emergency incident.

Emergency gates shall meet the specific requirements shown below:

5.20.5.1. Emergency gates shall be designed in accordance with applicable requirements for gates as stipulated in this Directive, section 5.3 & 5.4 as applicable.

5.20.5.2. Chain link gates for Class 1 & 2 facilities shall not be acceptable.

5.20.5.3. Emergency gates in the facility perimeter of facilities with a FSC of Class 1 or 2 shall be a single steel sliding or swing gate covering the full opening of the gate.

5.20.5.4. An emergency gate in the facility perimeter of Class 1 facilities shall be protected with an AVB that meets the requirements of AVB's as stated in SEC-06.

5.20.5.5. Concrete jersey barriers or removable bollards shall not be used as anti-vehicle protection for an Emergency Gate. FO shall use crash-rated beams or bollards, as specified in SEC-06, as AVB protection for an emergency gate where applicable.

5.20.5.6. FO shall implement a regular maintenance program for all manual or motorized Emergency Gates as specified in SEC-14.

5.20.5.7. Emergency gates shall have dedicated video surveillance that is monitored in the local SCC.

5.20.5.8. Gate width shall be at least 5m to allow the movement of emergency vehicles.

5.20.5.9. Emergency gates shall have the same anti-personnel and anti-vehicle characteristics, sensors and surveillance as facility perimeter fencing based on the FSC.

5.20.5.10. An Emergency Gate may be designed to accommodate abnormal, large & heavy equipment loads required to occasionally enter the facility.

6 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on its FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Preliminary Inspection Checkpoint (PIC)	✓	✓			
Vehicle Approach Speed Management (VASM)	✓	✓	✓	✓	✓
Auxiliary Gate	✓	✓	✓	✓	✓
Gatehouse	✓	✓	✓	✓	✓
Traffic Management	✓	✓	✓	✓	✓
Additional Inspection Vehicle Area	✓	✓			
Over Watch	✓	✓			
Support Building	✓	✓	✓	✓	
X-Ray & Inspection Building	✓	✓	✓		
Visitor Center	✓	✓	✓		
Communications	✓	✓	✓	✓	✓
Lighting	✓	✓	✓	✓	✓
Access Management	✓	✓	✓	✓	✓
Surveillance Cameras	✓	✓	✓	✓	
Response Zone	✓	✓			
Anti-Vehicle Barriers	✓	✓	✓	✓	
Power Systems	✓	✓	✓	✓	
Temporary Gate Closures	✓	✓	✓		

نسخة خاصة لشركة المياه الوطنية

7 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items. The Stage 3 submission, content and format are specified in SEC-14 section 6.3. This PoC shall form part of Section 14 of the Stage 3 submission package.

This PoC shall provide details for each of the requirements listed below.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-03 Reference	Requirement	FO Response
1.	5.1	Gate Design	*Provide the detail design drawings, with dimensions, for the detail layout of each gate in the facility perimeter as well as internal gates described in section 5.20.3.* *Drawings shall show all SEC-03 specified security elements*
2.	5.5	Gatehouse	*1. Provide the detail design drawings, with dimensions, for each of the gatehouses* *2. Provide design & installation specification document for the gatehouses* *3. Provide details and certifications for ballistic protection*
3.	5.10	Gate Support Buildings	*1. Provide the detail design drawings, with dimensions, for each of the gate support buildings* *2. Provide design & installation specification document for the gate support buildings* *3. Provide details and certifications for ballistic protection*
4.	5.12	Lighting	*1. Provide the detail design drawings, with dimensions, for the lighting layout of each gate in the facility* *2. Provide design & installation specification document for the gate lighting*
5.	5.20.5	Emergency Gate	*1. Provide the detail design drawings, with dimensions, for each of the emergency gates.* *2. Provide design & installation specification document for the emergency gate equipment*

8 Sample Drawings

This section contains sample drawings of various aspects of the Security Gate. These drawings are provided as conceptual drawings for the gate design. FO's shall meet the SEC requirements and submit site specific design drawings.

نسخة مرخصة لشركة المياه الوطنية

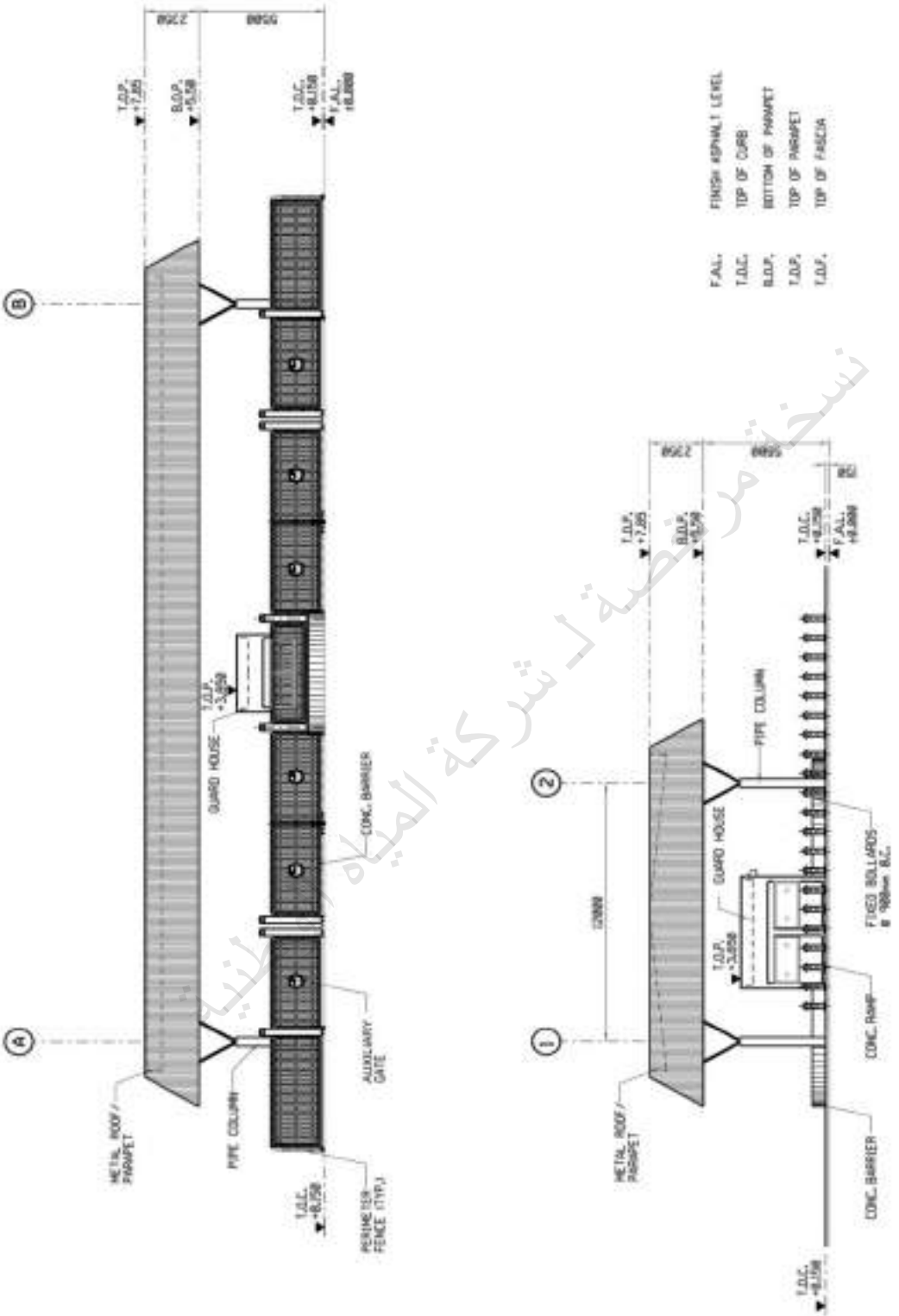


Figure 1: Main Gate

نسخة مرخصة لشركة المياه الوطنية

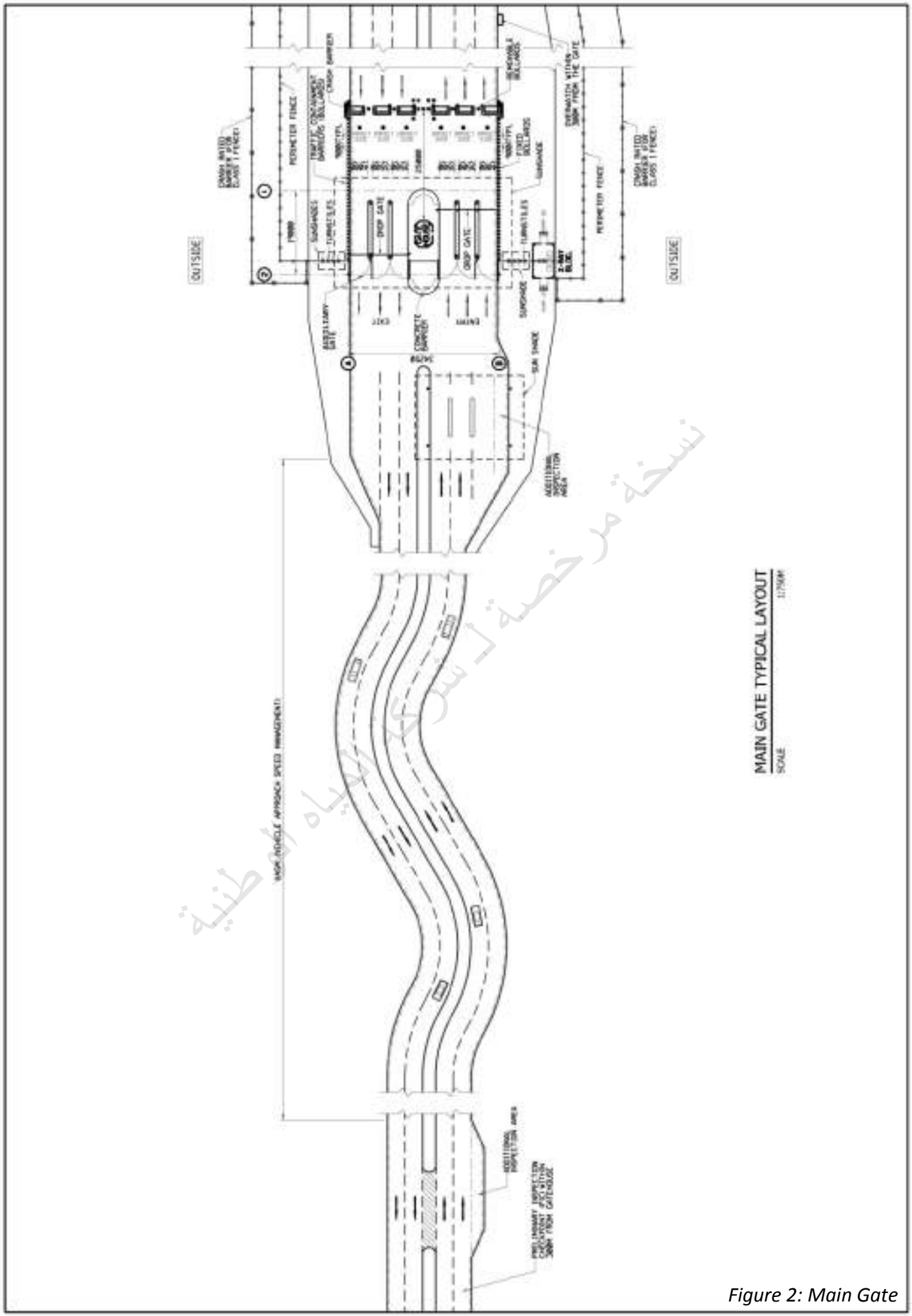


Figure 2: Main Gate

نسخة مرخصة لشركة المياه الوطنية

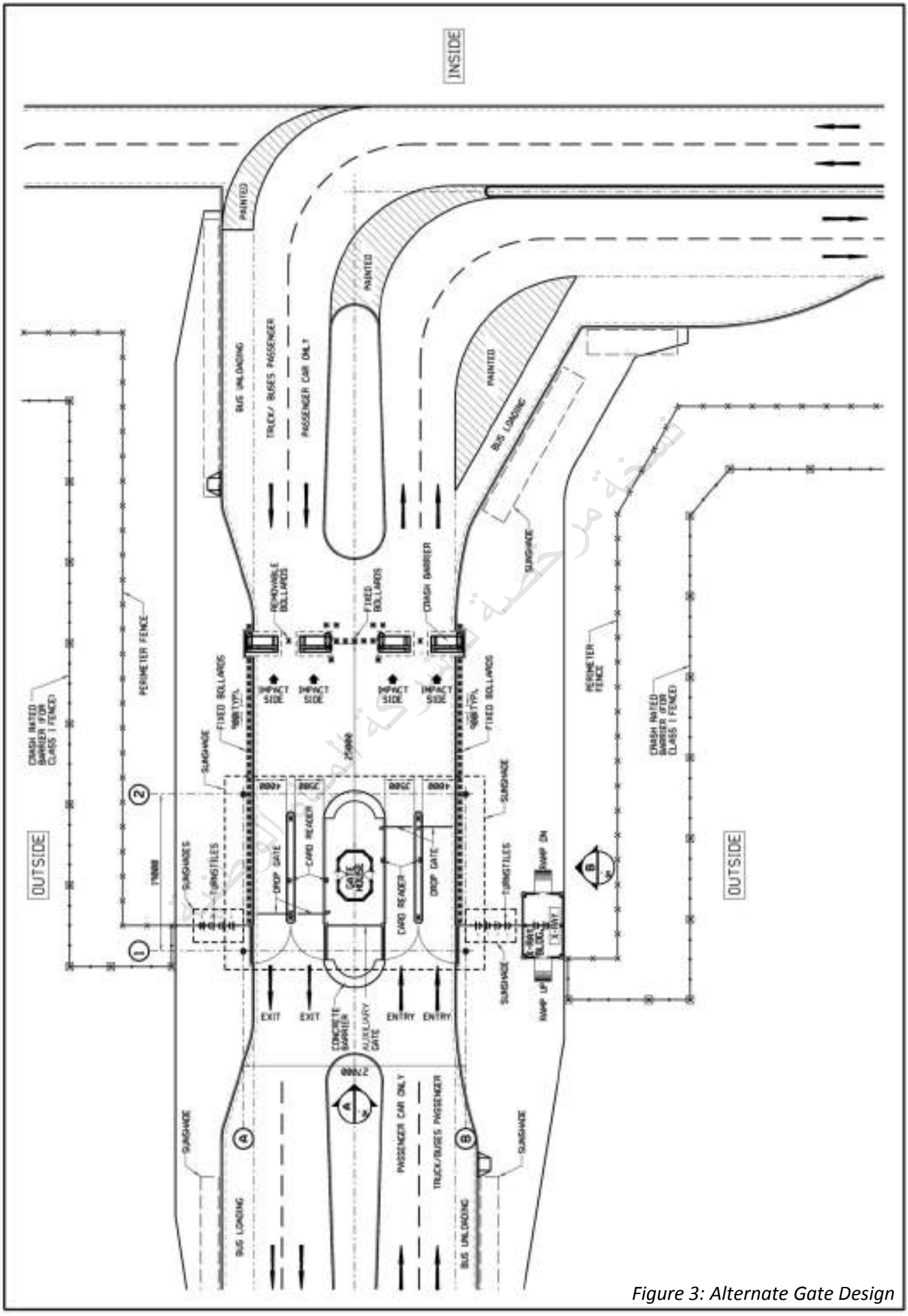


Figure 3: Alternate Gate Design

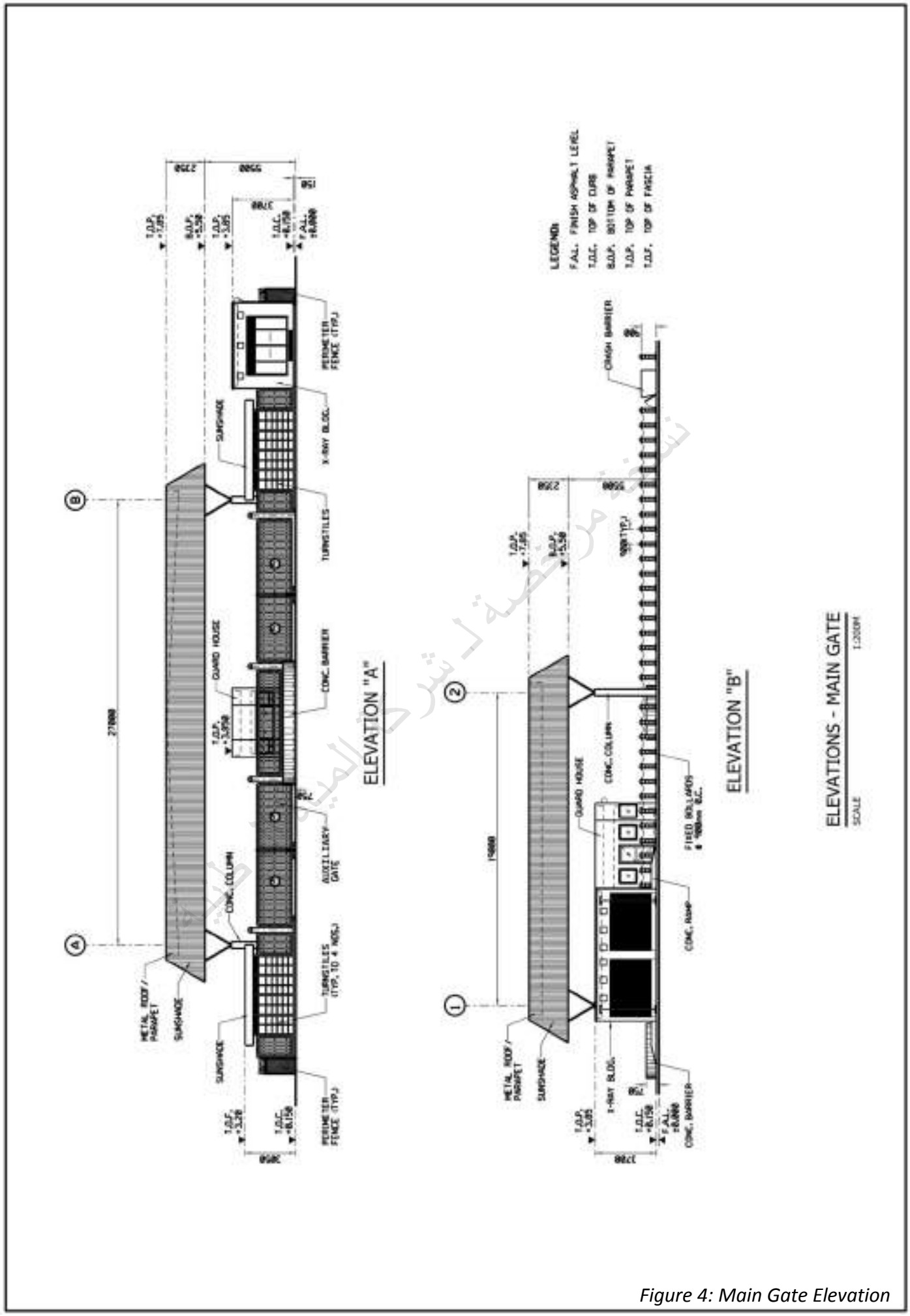


Figure 4: Main Gate Elevation

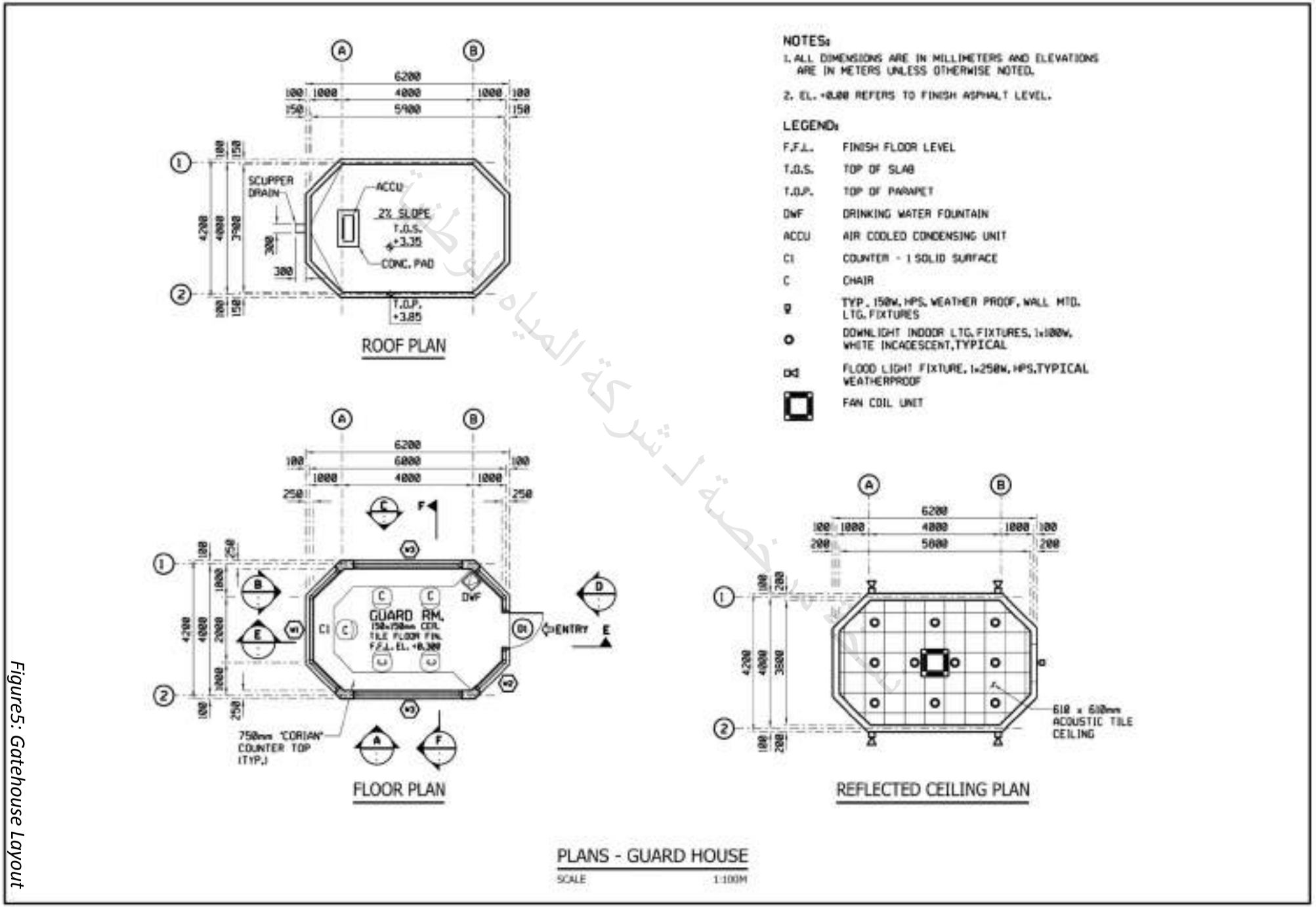


Figure5: Gatehouse Layout

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-04

Security Lighting

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7
2 SCOPE 7
3 ACRONYMS & DEFINITIONS 7
4 REFERENCES 7
5 GENERAL REQUIREMENTS 8
5.1 PERIMETER LIGHTING 8
5.2 AREA SECURITY LIGHTING 9
5.3 CHECKPOINT LIGHTING 10
5.4 GATE HOUSE INTERIOR LIGHTING 11
5.5 SHARED FENCE LIGHTING 12
5.6 COMMON REQUIREMENTS 13
5.6.1 Lighting System Design 13
5.6.2 Lighting Poles 14
5.6.3 Luminaire Requirements 14
5.6.4 Lamp Characteristics 15
5.6.5 Cabling 16
5.6.6 Power Supply 16
5.6.7 Lighting Control 17
5.6.8 Lighting System Maintenance 17
6 APPLICATION OF REQUIREMENTS 18
7 PROOF OF COMPLIANCE 19

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

The purpose of this Security (SEC) directive is to provide requirements for facility security lighting.

2 Scope

This directive specifies the different types of security lighting, lighting component selection requirements, cabling, power supply and lighting control.

3 Acronyms & Definitions

CRI	Color Rendering Index
FC	Foot Candles
HCIS	High Commission for Industrial Security
LDD	Luminaire Dirt Depreciation
LLD	Lamp Lumen Depreciation
Lumens	Système International d'unités (SI) unit of luminous flux
Lux	Système International d'unités (SI) unit of Illuminance
NEC	National Electrical Code
PCB	Polychlorinated Biphenyl
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation

4 References

This directive adopts the latest edition of the references listed.

ACI 318-05	*Building code requirement for structural concrete*
ASTM A123	*Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products*
IESNA Lighting Handbook	*The Illuminating Engineering Society of North America Lighting Handbook Reference & Application, 10th Edition (2011)*
IESNA RP-20	*Lighting for Parking Facilities*
NFPA 70	*National Fire Protection Association: National Electrical Code*
SEC-01	*General Requirements for Industrial Security*
SEC-02	*Security Fencing*
SEC-07	*Power Supply*
UL 1598	*Luminaires*

نسخة من هيئة الصناعات الأمنية

5 General Requirements

This Security Directive describes the general requirements for lighting at facilities. The types of lighting addressed in this Security Directive are as follows:

- Perimeter Lighting
- Area Lighting
- Check Point Lighting
- Gate House Interior Lighting
- Shared Fence Lighting
- Common Requirements

5.1 Perimeter Lighting

5.1.1. Perimeter lighting shall illuminate the fence line and its surrounding area with the minimum light levels shown below.

Lighting along the fence line shall be uniform with all light illumination overlapping adjacent light illumination. This measurement shall be taken 2 hours past sunset with existing facility lights turned off.

At no point along the fence line shall the illuminance be less than the values shown below:

5.1.1.1	Fence Line - *±1m*	23 lux
5.1.1.2	Fence Line - *3m inside*	20 lux
5.1.1.3	Fence Line - *10m outside*	12 lux

Shared fence lighting shall illuminate the fence line and its surrounding area with the minimum light levels shown in section 5.1.1.

If higher illuminance levels are required for operation of surveillance systems installed along the perimeter then the lighting system shall be designed for these higher levels. Perimeter lights shall be aimed to provide required illuminance.

5.1.2. Perimeter lighting shall have a maximum of 6:1 light-to-dark ratio with a minimum of 70% camera field of view illuminated.

5.1.3. Perimeter lighting shall be designed so that it shall not interfere with perimeter intrusion detection sensors, assessment cameras (such as glare, blinding or extreme bright spots within the camera field-of-view or the intrusion detection area), or be an aid to defeating the intrusion sensors.

نسخة مرخصة لشركة لمياء الوطنية

The lighting system shall be designed based on lighting calculations for the entire perimeter using the point by point method.

5.1.4. Poles used for installation of perimeter lighting shall typically be 5m high with the luminaire placed on top of the pole.

They shall typically be spaced at 20m intervals along the perimeter fence maintaining the requirements specified in 5.1.1 and 5.1.2. Regardless of actual pole height or spacing illuminance levels, as specified in this directive, shall be maintained along the entire perimeter.

5.1.5. Poles used for installation of perimeter lighting shall be setback from the fence as required by SEC-02 for the category of fence being used at the facility.

5.1.6. The lighting system shall be designed in accordance with the requirements of this Security Directive.

5.1.7. See Common Requirements in section 5.6 for additional requirements.

5.2 Area Security Lighting

Area security lighting shall illuminate designated areas. Designated areas are locations within the facility where illumination is required due to security considerations or SRA findings.

5.2.1 If higher illuminance levels are required for operation of surveillance systems installed at the facility then the lighting system shall be designed for these higher levels.

5.2.2 Lighting in the designated area shall be uniform with all light illumination overlapping adjacent light illumination. At no point in the designated area shall the average illuminance be less than 5 lux (0.5fc).

5.2.3 The illuminance in the designated area should be balanced with the illuminance in the surrounding area. In general, the luminance ratios should not exceed 8:1 but this may vary depending on local requirements.

5.2.4 Poles used for installation of area lighting shall be 10m to 30m high with the luminaire placed on top of the pole.

5.2.5 Area security lighting shall be spaced as required to meet the illuminance requirements.

5.2.6 Area lighting poles used at the perimeter fence shall be setback from the fence as required by SEC-02 for the category of fence being used at the facility.

5.2.7 Area lighting shall be designed so that it shall not interfere with perimeter intrusion detection sensors, assessment cameras (such as glare, blinding or extreme bright spots within the camera field-of-view or the intrusion detection area), or be an aid to defeating the intrusion sensors.

5.2.8 Area lighting design for parking facilities shall comply with IESNA RP-20.

5.2.9 See Common Requirements in section 5.6 of this Security Directive for additional requirements.

5.3 Checkpoint Lighting

5.3.1 Checkpoint lighting shall illuminate designated areas with the minimum light levels shown in section 5.1.1. Designated areas are the approach, exit and gatehouse area of the checkpoint or locations within the checkpoint where illumination is required due to operational considerations.

نسخة من خصخصة شركة المياه الوطنية

5.3.2 Lighting in the checkpoint area shall be uniform with all light illumination overlapping adjacent light illumination. At no point at the checkpoint, or area surrounding the gatehouse, shall the illuminance be less than the values shown below.

Illuminance at ground level: 100 lux (10fc)

OR

2 X Illuminance of the surrounding area.

Whichever is higher.

5.3.3 Vertical Illuminance: >25% of the horizontal illuminance at the level of vehicle driver.

The illuminance in the checkpoint area should be balanced with the illuminance in the surrounding area.

If higher illuminance levels are required for operation of surveillance systems installed at the checkpoint then the lighting system shall be designed for these higher levels.

5.3.4 Lights used for checkpoint Lighting shall have a CRI>50.

5.3.5 Light levels and luminaire aiming angles shall be sufficient to clearly identify incoming vehicles, vehicle license plates, pedestrians, vehicle drivers and cargo at least 20m away from the gate house anywhere in the checkpoint area and permit inspection of people, vehicles, goods and documents.

5.4 <u>Gate House Interior Lighting</u>

5.4.1 Gate House interior lighting shall provide adequate task level lighting with illuminance at the countertop level, inside the gate house, at least 300lux (30 fc).

5.4.2 Gate house interior lighting shall be selected to minimize reflections on the gate house windows.

5.4.3 A dimmer shall be provided for lights in each part of the gate house to allow intensity to be turned down in order to minimize gate house interior visibility from the outside.

5.4.4 Emergency lights shall be provided to enable operating personnel to follow planned operating and shutdown procedures in the event of a power failure.

5.4.5 All gate house lighting switch controls shall be installed at a single location.

نسخة مرخصة لشركة الهيئة الوطنية

5.5 Shared Fence Lighting

Shared fence lighting requirements apply when a new facility is set up next to an existing facility that already has perimeter lighting and intrusion detection. The intention of this requirement is to ensure that there is minimal interaction between the two facilities security systems and each security system functions independently of the other.

5.5.1 The new facility perimeter shall be lit with area lighting mounted on poles 10m to 30m high with the luminaire placed on top of the pole. This is used to eliminate any interference with the existing facility perimeter lighting.

5.5.2 Shared fence luminaires shall be mounted on top of poles with a vertical height selected so that the light output does not interfere with the cameras installed for the shared fence and perimeter cameras in the existing facility.

5.5.3 Poles used for mounting shared fence luminaires shall be setback a maximum of 10m from existing fence to meet the light levels specified in 5.2.2 & 5.2.3 of this directive.

5.5.4 The shared fence luminaire light output shall overlap existing facility lights on the fence line.

نسخة مرخصة لشركة المياه الوطنية

5.6 Common Requirements

This section describes requirements common to all security lighting.

5.6.1 **Lighting System Design**

The lighting system for perimeter, area lighting and shared fence lighting shall be designed based on lighting calculations using the point by point method.

5.6.1.1 Computer plotter prints shall be supplied with all security lighting proposals showing grid patterns and calculations covering perimeter, area lighting at perimeter fences and shared fence lighting.

5.6.1.2 Grid size on the plotter points shall be based upon a grid of 10 meters square while a grid of 3mx3m shall be used for perimeter lighting.

5.6.1.3 All calculation shall use a tarmacadam base reflectance factor of 0.01 in all lighting calculations. The uniformity of Illumination and the overall ratio of brightest to darkest regions in the designated area of interest shall meet the following minimum requirements unless otherwise specified:

Maximum to Minimum: 5:1
Average to Minimum: 2:1

5.6.1.4 The lighting in all areas shall be designed so that it does not interfere with cameras and does not intrude into the camera field of view to the extent that camera performance is affected.

5.6.1.5 At existing facilities, lighting output shall be measured and recorded. Measurements shall be taken 2 hours after local sunset. Shared fence lighting has special requirements for this measurement as specified in 0section 5.5.

5.6.1.6 Lighting design for parking facilities shall be in accordance with IESNA RP-20.

5.6.2 **Lighting Poles**

5.6.2.1 Poles shall be made of aluminum or hot-dipped galvanized steel.

5.6.2.2 The pole design shall be selected on the basis of structural integrity and corrosion protection within the selected environment.

5.6.2.3 Steel poles shall comply with ASTM A123 for corrosion protection. All fasteners used on poles, and pole components, shall be protected against corrosion.

5.6.2.4 Aluminum poles shall be suitably protected inside and outside against damage by environmental elements.

5.6.2.5 Each pole shall have an environmentally sealed wiring compartment for connecting to the power system.

5.6.2.6 The wiring compartment shall be sealed against vermin or moisture ingress.

5.6.2.7 The pole shall be grounded in accordance with NFPA 70.

5.6.2.8 The foundation for the poles shall be designed to carry the weight of the poles and withstand wind effects on the entire assembly.

The foundations for lighting poles shall comply with the requirements of ACI-318, or equivalent, for such foundations.

5.6.2.9 FO shall ensure that the pole assembly is damped against wind or seismic induced vibrations.

5.6.3 **Luminaire Requirements**

5.6.3.1 Each luminaire deployed for compliance with this standard shall have a LLD of 0.90 & LDD of 0.71 or better.

5.6.3.2 The luminaire body and frame shall be made of corrosion resistant material such as, but not limited to, die cast aluminum. Supplier shall provide data on which internationally recognizable standard for corrosion protection has been used in the manufacture of the luminaire.

5.6.3.3 Luminaires shall be watertight and sealed against water or dust ingress.

5.6.3.4 The luminaire shall be certified to comply with the requirements of UL 1598 for wet locations. Equivalent standards may be used where they provide similar protection.

5.6.3.5 Luminaires shall be certified by the manufacturer for operation in the environmental conditions stated in SEC-01.

5.6.3.6 Luminaires used in marine environments shall be specifically designed for such environments and shall be certified by the manufacturer.

5.6.3.7 The luminaire shall be designed so that it can be aimed in both horizontal and vertical directions.

5.6.3.8 Luminaires installed at the perimeter shall have an asymmetric forward throw beam (unless otherwise stated) with a wide beam angle to cover designated areas.

The beam spread shall be such that adjacent beams overlap and eliminate any dark areas in the area of interest.

5.6.3.9 The lens shall be heat and impact resistant. It shall be hinged for easy access or complete removal.

5.6.3.10 The luminaires shall be of full cut-off design in order to direct light to the area of interest and minimize upwards light spill.

5.6.3.11 The luminaire shall be grounded in accordance with NFPA 70.

5.6.3.12 The use of energy-efficient luminaires like LED, metal halide, high-pressure sodium and fluorescent shall be maximized where possible.

5.6.3.13 FO shall provide HCIS with test reports to verify luminaire performance.

5.6.4 **Lamp Characteristics**

5.6.4.1 FO may use any lighting technology as long as all light levels at designated distances are maintained.

5.6.4.2 Luminaires used in coastal, or other areas, subject to fog and low clouds should use light sources specifically designed for use in such environments.

5.6.4.3 All luminaire components shall be certified by the manufacturer as being PCB free.

5.6.4.4 All luminaire components shall be certified by the manufacturer as being fully functional under the environmental conditions stated in SEC-01.

5.6.4.5 The restrike time for (for different areas/applications) all security lighting shall be under 20 minutes under all conditions in all security lighting applications.

FO shall implement measures to maintain perimeter integrity and detection capability during the restrike time when the lamp is not at full illumination.

5.6.5 **Cabling**

5.6.5.1 Cabling shall be buried in accordance with NEC requirements.

5.6.5.2 Where cables rise above ground they shall be protected by rigid steel conduit or by rising inside the support masts for the lights.

5.6.5.3 Cables shall comply with applicable electrical codes stated in NFPA-70.

5.6.6 **Power Supply**

Perimeter Lighting

5.6.6.1 In Class 1 & 2 facilities, two dedicated power supplies shall be used to power perimeter lights. Each circuit shall be setup in a loop design similar to a domestic ring main configuration.

5.6.6.2 Each light shall be on an individual circuit from the ring main.

5.6.6.3 Each light shall be connected to a different ring main than the light adjacent to it.

5.6.6.4 Lights shall be powered by the emergency power generator in the event of power failure.

5.6.6.5 Each lighting fixture shall be protected by a fuse or circuit breaker in a secure compartment with a suitable lock.

نسخة مرخصة لشركة المياه الوطنية

5.6.6.6 The power supply shall fully comply with the requirements stated in SEC-07.

Other Lighting

5.6.6.7 Power supply for security lighting, other than Perimeter Lighting defined in 0, shall fully comply with the requirements of SEC-07.

5.6.7 Lighting Control

5.6.7.1 Perimeter, area lighting, checkpoint lighting and shared fence lighting shall be controlled automatically. The lighting controls shall be designed so the lights are energized prior to darkness, or during the day, at a time suitable for the run-up period of the lamps used.

5.6.7.2 Lighting controls shall energize the lights when the ambient natural lighting level is 1.6 times the average horizontal perimeter light illuminance design level or 15 lux (1.5fc), whichever is higher.

This ensures that the designed illuminance is met during dark periods of the day as well as at dusk and after dark.

5.6.7.3 A manual backup switch to power on perimeter lighting shall be provided in the SCC. Where there is no local SCC, the switch shall be installed in a secured location as specified in section 5.6.7.6.

5.6.7.4 A switch shall be provided in the SCC to permit the use of alternate perimeter, area or shared fence luminaires if required. Activation of this switch shall cause every alternate luminaire to turn on.

5.6.7.5 Security lighting shall be independent of other lighting and power systems at the facility.

5.6.7.6 All switchgear controls and switches for security lighting shall be located in a locked and secure facility.

5.6.8 Lighting System Maintenance

5.6.8.1 The FO shall initiate procedures to detect failed lights by periodic review of all cameras and implementing procedures for vehicle patrols to report failed lights.

5.6.8.2 FO shall implement a lighting system maintenance program. This program shall be fully documented and comply with lighting system maintenance requirements specified in SEC-15.

6 Application of Requirements

This section lists how the elements of this security directive apply to facilities depending on their FSC as specified in SEC-01 Appendix A.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Perimeter Lighting	✓	✓	✓		
Area Security Lighting	✓	✓	✓	✓	
Checkpoint Lighting	✓	✓	✓	✓	✓
Gatehouse Interior Lighting	✓	✓	✓	✓	✓
Shared Fence Lighting	✓	✓	✓		
Common Requirements	✓	✓	✓	✓	✓

نسخة مرخصة لشركة المياه الوطنية

7 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-04 Reference	Requirement	FO Response
1.	5.1.4 & 5.6.1	Lighting System Design basis	*Submit lighting calculations methodology & results for all security lighting in all areas of facility*
2.	5.1 & 5.6.2	Perimeter Lighting	*Submit data sheets & drawings to show pole details and layout at fence line.*
3.	5.2 & 5.6.2	Area Lighting	*Submit data sheets & drawings to show pole details and layouts.*
4.	5.3	Checkpoint Lighting	*Submit data sheets & drawings to show lighting layouts* *Submit luminaire data to show CRI rating and illumination capacity*
5.	5.5	Shared Fence Lighting	*Submit data sheets & drawings to show lighting layouts* *Submit luminaire data to show illumination capacity*
6.	5.6.3	Luminaire	*Submit data sheets for all luminaires selected for security lighting* *Show LDD for all luminaires*
7.	5.6.4	Lamp	*Submit lamp data sheets for each application* *Show LLD for all lamps*
8.	0.1.	Power Supply	*Provide drawings showing cabling for perimeter lighting at category 1 & 2 facilities only.*
9.	5.6.7	Lighting Control	*Provide overview of lighting control systems and locations of any manual switches.*
10.	5.6.1.5	Lighting Levels	*Actual lighting levels shall be measured & recorded 2 hours after sunset and provided to HCIS*

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-05

Security Systems at Industrial Facilities

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7

2 SCOPE 7

3 ACRONYMS & DEFINITIONS 7

4 REFERENCES 8

5 GENERAL REQUIREMENTS 9

5.1 Required Security Systems 9
5.2 System Design Constraints 9
5.3 Access Control System 12
5.4 Automatic License Plate Recognition System 18
5.5 Intrusion Detection & Assessment System 20
5.6 ID Management System 26
5.7 Video Assessment & Surveillance System 26
5.8 Camera Specifications 29
5.9 Plant Control Room 30
5.10 Integration Requirements 31
5.11 Security Control Center 31

6 APPLICATION OF REQUIREMENTS 33

7 PROOF OF COMPLIANCE 34

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

The purpose of this Security (SEC) directive is to provide requirements for the deployment of security systems at industrial facilities under the jurisdiction of the HCIS.

2 Scope

This Directive provides the minimum requirements for companies and establishments that are subject to the supervision of the High Commission for Industrial Security (HCIS), Ministry of Interior, for security systems used at industrial facilities.

3 Acronyms & Definitions

ACS	Access Control System
ALPR	Automatic License Plate Recognition System
CPU	Central Processing Unit
CR	Card Readers
ERP	Emergency Response Plan
FO	Facility Operator: the owner, operator or lessee of a facility
FOV	Field of View
FSC	Facility Security Classification
GCC	Gulf Cooperation Council
GIS	Geographic Information System
HCIS	High Commission for Industrial Security
HD	High Definition television
HDD	Hard Disc Drive
IDAS	Intrusion Detection and Assessment System
IDMS	Identification Card Management System
LAN	Local Area Network
LRS	Long Range Surveillance
LWIR	Long Wave Infra-Red
OCR	Optical Character Recognition
OS	Operating System
PCR	Plant Control Room
PIN	Personal identification Number
PIV	Personal Identification Verification Card
PoC	Proof of Compliance
PTZ	Pan-Tilt-Zoom
SCC	Security Control Center
SED	Single Entry Device
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
SRA	Security Risk Assessment
SSD	Solid State Disc
UPS	Uninterruptible Power Supply
VASS	Video Assessment & Surveillance System

نسخة مرخصة لـ [illegible]

4 References

This directive adopts the latest edition of the references listed.

ANSI/SIA CP-01-2014	*American National Standard Institute/Security Industry Association – False Alarm Reduction Standard*
IEC 60529	*Degrees of protection provided by enclosures (IP Code)*
ISO 110641-1	*Principles for the Design of Control Centers*
ISO 110641-2	*Principles for the Arrangement of Control Suites*
ISO 110641-3	*Control Room Layout*
ISO 110641-4	*Layout & Dimensions of Work stations*
ISO 110641-5	*Display and Controls*
ISO 110641-6	*Environmental requirements for Control Centers*
ISO 110641-7	*Principles for the Evaluation of Control Centers*
SAF-04	*Fire Protection Systems and Equipment*
SAF-20	*Pre-Incident Planning and Management of Emergencies*
SEC-01	*General Requirements for Security Directives*
SEC-02	*Security Fencing*
SEC-04	*Security Lighting*
SEC-06	*Security Devices*
SEC-07	*Power Supplies*
SEC-08	*Security Communications and Data Networks*
SEC-09	*Structures housing Security Equipment*
SEC-11	*Identification Cards*
SEC-12	*Cyber Security*
SEC-15	*Security Management at Industrial Facilities*

5 General Requirements

Industrial facilities, under the jurisdiction of the HCIS, shall install security systems at each industrial facility and integrate them into an integrated operating environment at a SCC.

This directive provides the specific requirements for each required security system and the integration requirements at the SCC.

5.1 Required Security Systems

The following security systems shall be installed at each facility as required by the facility FSC:

- Access Control System (ACS)
- Automatic License Plate Recognition System (ALPR)
- Intrusion Detection & Assessment System (IDAS)
- ID Management System (IDMS)
- Video Assessment & Surveillance System (VASS)

5.2 System Design Constraints

All security systems shall meet the constraints and requirements stated in this section.

5.2.1 **Single Point of Failure**

Security systems shall be designed so that no single component failure can disable the system.

5.2.2 **Redundancy**

Security system computers shall be installed in a redundant configuration with primary and backup computers.

Failover from the primary to the backup computer shall be automatic with no loss of data.

FO may use fault-tolerant computers that utilize built-in hardware to provide automatic switchover from failed components in lieu of a primary/backup configuration. However, such devices must cover all computer components such as CPU, memory, power supply, network, etc.

نسخة من خصة - شركة المياه الوطنية

5.2.3 Hardware

Computer hardware used for security systems shall be of the latest generation available at the time of the design completion. The hardware shall have adequate memory and processing capacity to ensure fast response to system requirements and user commands.

Operating system and applications shall be installed on a HDD or SSD while data shall be stored on a separate discrete physical HDD or SSD. Disc capacity shall be sized to maintain at least 50% spare capacity beyond expected system requirements.

5.2.4 Operating Systems

The OS used for security system implementation must be current and have full mainstream support from the manufacturer.

All current service packs, and other OS updates, shall be installed at the time of system delivery.

FO may not use an OS for security systems that has been superseded by a newer version released by the OS manufacturer.

5.2.5 Communications & Data Networks

Communications & data networks used in security systems shall be fully compliant with SEC-08 and SEC-12.

5.2.6 Database

All data pertaining to each security system shall be stored in a relational data base management system. The system storage shall be sized to ensure that all system data is available online for the retention period specified in other sections of this directive for each required system.

5.2.7 Data Backup

All system data pertaining to the security system shall be backed up on a regular schedule. This schedule shall include daily, weekly and monthly backups.

Incremental data backup may be on a daily basis but a full backup must be taken at least once every 30 days. The data backup shall be stored locally and

also at an offsite location for disaster recovery. Access to the data backup shall be limited to authorized users.

5.2.8 **External Systems Interface**

All security systems shall have a clearly defined, and documented, procedure for providing all system data, including video, to an external system for display and acknowledgement if required by FO or operational requirements.

This data shall be made available to the external system after full compliance with security authentication protocols.

All data transmitted to an external system shall use encryption, in accordance with the requirements of SEC-08 and SEC-12, to secure the data during transit over the network.

5.2.9 **Security**

All security system installations shall follow SEC-08 requirements for data networks and SEC-12 requirements for cybersecurity to protect the system against unauthorized access attempts.

5.2.10 **Power Supply**

All security systems shall be powered by an uninterruptible power supply, backed up by an emergency power generator, fully compliant with SEC-07.

5.2.11 **Environmental**

All security system devices and components mounted outdoors shall be sealed to a minimum standard of IEC 60529 and shall be rated for operation in the environmental conditions stated in SEC-01.

Indoor devices shall have air conditioning compliant with SEC-01.

5.2.12 **Installation & Maintenance**

Structures that house security systems shall meet the requirements of SEC-09. Systems shall be maintained pursuant to the requirements of SEC-15.

5.2.13 **Date/Time Synchronization**

All devices connected to the security systems shall have their date/time synchronized to each other. In general, time synchronization shall be based on the date/time setting at a single central location determined by the FO.

5.2.14 **Tamper Protection**

All security systems shall incorporate elements that will annunciate an alarm if any attempt is made to tamper with system elements such as cabling, computer equipment or field computer facility access where active system components or terminations are located.

All junction & pull boxes, mounted externally, shall use tamper-proof screws for all fasteners on the case that are externally accessible.

No cabling shall be visible externally and all openings into system housings shall be sealed.

All surface mounted cables shall be encased in steel conduit.

5.3 Access Control System

The ACS comprises the hardware and software needed to electronically authenticate a request by personnel to access a facility and to notify security personnel of any invalid attempts.

The ACS shall meet the following requirements:

5.3.1 **Architecture**

5.3.1.1 The ACS shall consist of a local ACS at each facility with a central ACS that shall store and retain all ACS personnel and access data online for at least 36 months.

5.3.1.2 Personnel data referring to card holder short leave, vacation, lost, stolen or revoked status shall be automatically updated in the ACS and disseminated automatically to all ACS sites.

Personnel data updates shall be carried out in secure fashion.

5.3.1.3 All local ACS operations & functions shall continue to operate with no loss of capability when communication links to the central ACS are disrupted.

5.3.1.4 All local access data shall be uploaded to central system at periodic intervals not to exceed 10 minutes.

5.3.1.5 System shall protect against tail gating.

5.3.1.6 Local & Global anti-pass back shall be enforced by the system. This shall prevent a card holder from making an entry unless an exit has already been recorded in the system.

نسخة مرخصة لشركة المياه الوطنية

5.3.1.7 FO shall ensure that non-security related access to the ACS, or ACS data, shall not be permitted.

5.3.2 Card Readers or Biometric Readers

Card Readers (CR) or biometric readers shall be used to initiate a request for access at a SED associated with the CR. The CR shall display the ACS response and unlock the associated SED.

5.3.2.1 One CR may control only one SED.

5.3.2.2 Where the installation only has one SED for both entry and exit, two CR's shall be installed, on both the entry and exit sides of the SED, to allow continued operation if one of the CR's fails.

5.3.2.3 If CR controllers are used a minimum of two controllers shall be installed with each alternate CR connected to alternate controllers.

5.3.2.4 The ACS shall have the ability to deploy CR's in multiple zones with each zone having independent security access levels.

5.3.2.5 The CR shall allow or deny access based on the response from the ACS. All access denied alarms shall be annunciated at the local gatehouse.

5.3.3 Card Readers

CR's shall be able to read PIV cards configured according to the requirements of SEC-11.

CR's shall incorporate PIN keypads. The ACS shall use the PIV and 4 digit minimum PIN entry or PIV and biometric read to verify access rights which shall be validated by the ACS.

PINs shall be machine generated using a random or pseudo random algorithm and must be changed every 6 months. FO shall ensure that procedures are in place to notify users of PIN changes.

5.3.4 Biometric Readers

Biometric readers may use fingerprint, hand geometry, iris or any other biometric measurement generally accepted within the security industry and fully compliant with SEC-11.

Biometric readers shall validate data against a biometric template either stored in a smart card or against a central database. Biometric data retained in the smart card shall be encrypted as specified in SEC-11.

All biometric readers shall have the ability to verify that the measurements are being taken from a live person and not a printed copy or a copy made from some inanimate object.

5.3.5 Reader User interface

CR's & biometric readers shall communicate access request status to users as follows:

The device shall have indicators to inform the user that the device is ready, access request is being processed, request approved or request denied. If indicator lights are used they shall use different colors for request approval and denial.

Displays or indicators used in such devices shall have clearly visible displays in bright daylight conditions. Where displays are used for textual information to the user, the fonts and stroke weight shall be adequately sized to allow reading by users.

The system shall allow entry of a duress code on the card reader keypad to inform the ACS about an access attempt being made under duress.

5.3.6 Single Entry Device

The SED refers to the device used to control access to and from the facility. For personnel it is generally a turnstile and for vehicles it is a drop arm barrier or deployable anti-vehicle barrier. The SED shall be controlled by the ACS and shall normally be in closed or locked position unless released by the ACS after an authenticated PIV or biometric read.

All SED's shall be compliant with SEC-06.

5.3.7 Alarm Annunciation

The ACS shall utilize displays and printers to annunciate alarms and keep security personnel apprised of system and access request status. All displays and printers shall be mounted in local gatehouse with the option to remotely annunciate the alarms at an external system.

The system shall require acknowledgement by security personnel of each alarm.

Devices used for alarm annunciation are as follows:

Status Display

Displays overall system diagram and status of each device using colors to denote system status.

Display shall include status of local computers, communication links (if any), UPS status, access request status. All titles shall be bilingual in Arabic & English.

Alarm Display

Display status of access request with configurable option to display selected events.

Display shall include critical access denied messages in color. All messages shall be bilingual in Arabic & English.

Printer

Print hardcopy, line by line, of all messages on Alarm Display.

Operator shall have option to use, or not use, the printer but the function shall be provided.

Printer shall continue to operate, and print required messages, regardless of communication link status.

Audio Alarm Annunciation

All alarm messages shall be accompanied by an audio tone that shall be audible above ambient noise in the gatehouse.

A distinct audio tone shall be used when an alarm is generated due to an access attempt by a card that is marked lost, stolen, revoked, on vacation, expired or duress code entry.

Response Time

The alarm annunciation system shall respond to a valid/invalid access attempt in less than 0.5 seconds and display any alarm condition.

Operation

All displays shall continue to operate, and display complete system information, regardless of communication link status from the local ACS to the central ACS.

نسخة مرخصة لشركة ليان الوطنية

5.3.8 **Emergency Release**

Emergency Release refers to a physical emergency switch that will allow security personnel to initiate an emergency deployment of pre-selected SED's when required.

5.3.8.1 Emergency Release switch shall be protected against accidental activation.

5.3.8.2 Only pre-selected single entry devices shall be deployed or locked.

5.3.8.3 Emergency switch activation shall be logged in ACS.

5.3.8.4 Emergency switch shall function independently of the ACS.

5.3.8.5 In the event of an emergency, gate personnel shall be permitted to allow entry and exit of emergency vehicles.

5.3.8.6 The ACS shall permit gate personnel to initiate emergency procedures to allow the free exit of facility personnel under emergency conditions. As part of these procedures the ACS shall provide the facility to update personnel access status as the actual data is collected during an emergency.

5.3.9 **ACS Cameras**

The ACS shall include cameras to record ACS users and general gate area surveillance.

Gate Surveillance: 1 fixed camera for entry side and 1 fixed camera for exit side that monitors the approaches to the turnstiles.

Gate Assessment: 1 PTZ color camera for entry side and 1 PTZ color camera for exit side that allows the operator to monitor different gate areas and zoom in as needed.

User: 1 fixed camera at each CR.

5.3.9.1 All ACS cameras shall comply with the requirements stated in section 5.8 of this directive.

5.3.9.2 User cameras shall meet the following requirements:

- Adequate wide-angle capability to display a recognizable image of the user of the CR, for a height range (of the user) of 1.3-2.2 m.
- The camera shall be positioned to minimize the possibilities of user obscuring a view of the face.

- The FO shall site the user camera to obstruct keypad view while maintaining the ability to see faces of personnel entering the facility.
- User camera images shall only be triggered by an access request. A two (2) second video of the user shall be recorded initiating with the card swipe.

5.3.9.3 The system shall have the ability to display cameras imagery locally and/or remotely as required by the FO.

5.3.9.4 The system shall annunciate an alarm when the video signal from the image is lost.

5.3.10 **Video Recording**

All images from ACS cameras shall be recorded and retained for the intervals specified below, from the date the image was recorded, before the data can be overwritten.

- Gate Surveillance; 90 days
- Gate Assessment; 30 days
- User; 90 days

The video from all ACS cameras shall be stored and available for viewing, locally and across the security network by authorized users.

5.3.11 **Reporting Requirements**

The ACS shall provide a set of reporting tools that shall allow authorized system operators and gate personnel to generate reports from data stored in the ACS database. The following pre-formatted reports shall be available for ACS personnel to generate at any time:

5.3.11.1 On-Site Report: Lists all personnel on site with details of last access point used, department name & contact numbers for each person.

5.3.11.2 Visitor Report: Lists all visitors to site. This report shall include, at a minimum, visitor name, organization being visited, contact person, exit / entry dates/time, gates used.

5.3.11.3 Card holder photographs and access records shall be available on the local system for review by gate and SCC personnel.

5.4 Automatic License Plate Recognition System

The ALPR System consists of cameras and illuminators, connected to the ALPR computer system, at each vehicle traffic entry lane in a Class 1, 2 or 3 facility. It detects incoming vehicle license plates, recognizes all plate characters, validates them against a stored list and annunciates an alarm when a discrepancy is detected.

The ALPR System shall comply with the following requirements:

- ALPR System architecture
- License plate database
- Cameras
- Illuminators
- Optical Character Recognition System
- Alarm annunciation system

5.4.1 **ALPR System Architecture:**

5.4.1.1 The IDMS shall consist of local ALPR workstations at a facility with a central server for ALPR data storage and management.

5.4.1.2 All computer hardware, and support equipment, shall comply with the system constraints specified in section 5.2 of this directive.

5.4.2 **License Plate Database**

5.4.2.1 The main ALPR database shall be located on the central server with local databases at each gate using ALPR systems.

5.4.2.2 This main ALPR database shall contain data on license plates that are suspect or are not permitted into facilities.

5.4.2.3 FO shall coordinate with local traffic authorities to acquire license plate updates on stolen vehicles or other vehicles of interest to the authorities. These updates shall be copied to the main ALPR database by the 1st working day after receipt.

5.4.2.4 FO shall update the database with license plates of personnel considered persona non grata for entry into the facilities.

5.4.2.5 Updates shall be made to the database on a daily basis and shall be transmitted to all gates with ALPR systems within 1 hour of update completion.

نسخة مرخصة لشركة المياه الوطنية

5.4.3 Cameras

5.4.3.1 ALPR cameras shall be installed in all Class 1, 2 and 3 facility Main Gate entry traffic lanes.

5.4.3.2 The cameras shall be located a maximum of 50m from the entry side Main Gate gatehouse on the external side where traffic is approaching.

5.4.3.3 There shall be adequate distance to allow the ALPR system to read and validate a license plate and annunciate an alarm before the vehicle reaches the gatehouse.

5.4.3.4 The cameras shall either be custom made for ALPR application or shall have adequate resolution, and other characteristics, to meet ALPR requirements.

5.4.3.5 Camera shall have the following performance characteristics:

- Shutter speed shall be set to 1/1000 of a second to avoid image blurring.
- Uses the appropriate shutter type to avoid distortion.
- Cameras shall have automatic exposure and iris controls to deal with changing ambient light conditions.
- Cameras shall be able to distinguish colors used in license plates.

5.4.3.6 Camera shall be carefully sited relative to the target capture area. Care shall be taken to ensure that angles of incidence between camera lens and license plate shall be selected to minimize distortion and ensure usable images.

5.4.3.7 The camera depth of field shall be maintained within acceptable ranges to ensure clear images.

5.4.3.8 Cameras shall comply with the environmental requirements of SEC-01.

5.4.4 Illuminators

5.4.4.1 License plate illuminators shall be co-located with the ALPR camera to ensure uniform illumination of the target area.

5.4.4.2 Illuminators may either be visible light or infrared as needed to ensure clear images.

5.4.4.3 The illuminators shall be angled to minimize discomfort to approaching drivers.

5.4.5 Optical Character Recognition System

5.4.5.1 The ALPR system shall incorporate OCR capability to extract all relevant data, including colors, from the license plate image. This extraction shall be fully automatic and take place without any user intervention.

5.4.5.2 The ALPR system shall recognize all license plates from all GCC countries. Changes in license plate layouts shall be updated in the system within 15 days of the release of the new license plates formats or content.

5.4.6 Alarm Annunciation System

5.4.6.1 The ALPR system shall automatically annunciate alarms in the local gatehouse and the facility SCC.

5.4.6.2 The alarm detail shall be accompanied by audio and visual indicators. The audio shall have distinct characteristics while the visual indicators may be a flashing light in the gatehouse or relevant traffic lane.

5.4.6.3 Alarm details shall be displayed to both gate & SCC personnel.

5.4.6.4 Alarm may be annunciated on a dedicated display or, if technically feasible, on a display shared with other systems.

5.4.6.5 In all cases, alarms must be acknowledged by gate personnel.

5.5 Intrusion Detection & Assessment System

The IDAS consists of sensors and imaging systems at the facility perimeter that are connected to the IDAS computer system. This system analyzes and localizes sensor data, triggers an alarm when an intrusion is detected, displays pre & post alarm live video from the camera covering the area where the alarm was triggered, slews an assessment camera to the detection location and displays assessment camera imagery to an operator.

The major components of an IDAS are as follows:

- Cameras & Sensors
- Alarm Detection & Annunciation
- User Interface & Displays
- Performance Requirements

5.5.1 Cameras & Sensors

Cameras and sensors are deployed around the facility perimeter fence as specified in SEC-02.

Cameras

5.5.1.1 All IDAS cameras & sensors shall be geospatially mapped so that their location, and imagery, can be accurately displayed on a GIS map.

5.5.1.2 Camera specifications may be found in section 5.7. & 5.8 in this directive.

5.5.1.3 The IDAS shall use two separate camera types:

- Perimeter Surveillance: Fixed cameras that permit constant monitoring of the section of perimeter being covered by the camera.
- Perimeter Assessment: PTZ cameras that automatically slew to an alarm location within their covered area.

Cameras may be optical and/or thermal as required by the SRA.

5.5.1.4 Cameras shall have auto adjustment capability to adapt to varying lighting and environmental conditions.

Sensors

The IDAS shall use at least 2 independent types of sensors to detect an intrusion attempt into the facility. The general requirements of sensors are as follows:

5.5.1.5 Multi-spectral sensors shall be used to detect intrusions using different parts of the electromagnetic spectrum.

5.5.1.6 Sensors shall be adjustable to set detection thresholds.

5.5.1.7 One of the sensors shall detect an intrusion attempt at a specific point.

5.5.1.8 A volumetric sensor shall detect any motion, within the covered volume, of any man sized object on the inside of the anti-personnel fence.

5.5.1.9 Sensors shall not be degraded in intense fog levels, rain or during a sandstorm.

5.5.1.10 Sensors shall be deployed in the locations specified in SEC-02.

5.5.1.11 The effective sensitivity of all sensors shall be uniform in the entire area/volume being monitored by the sensors. Where variable

sensitivity is employed, FO shall ensure that the sensitivity is adequate in all locations in the sensor volume, including the edges.

5.5.1.12 Sensor overlap shall be used to cover areas at the sensor coverage edge to ensure elimination of any blind spots.

5.5.2 Intrusion Detection & Annunciation

Intrusions shall be detected by the sensors and annunciated at a local or, if required by FO, remote SCC.

Intrusion Detection

FO may use discrete sensors, as specified above, for intrusion detection or may use the perimeter surveillance fixed cameras as one of the intrusion sensors. Where the fixed cameras are used as one of the intrusion sensors the following conditions apply:

5.5.2.1. Sensor must be effective in all weather conditions including fog, rain or sandstorms.

5.5.2.2. Camera imagery shall utilize a Video Analytics System, as specified in section 5.7.3, to detect an intrusion attempt by analysis of the incoming video.

Alarm Annunciation

The IDAS shall annunciate the alarm locally or, if required by the FO, at a remote SCC.

5.5.2.3. Alarm annunciation shall use a GIS map to display accurate alarm location data.

5.5.2.4. The SCC shall be capable of receiving the alarm data & video and sending back an acknowledgement to the IDAS system.

5.5.2.5. Regardless of the existence of a remote SCC, the local users shall have the ability to interact with the system and manage all alarms.

5.5.2.6. The alarm displays shall display all alarm indications in all detection zones as well as individual device status.

5.5.2.7. All device or component failures shall be annunciated on alarm displays at the facility where the system is installed.

5.5.2.8. If the system uses remote management then these alarms shall also be displayed at the remote SCC.

5.5.2.9. System shall incorporate alarms about faults within the system such as, but not limited to, elevated temperatures in equipment

rooms, device failures or communication failures between system and sensors.

5.5.2.10. When an alarm occurs the IDAS shall immediately switch a designated display to playback pre alarm video and live video from the alarmed zone cameras.

5.5.2.11. The Perimeter Assessment camera shall be automatically slewed to the alarm zone to allow further assessment by the operators.

5.5.3 User Interface & Displays

5.5.3.1 ***CCTV Interface***

The IDAS shall provide a full set of controls as generally used in CCTV systems. This will allow the IDAS user to select cameras for display, use split screens, manage PTZ cameras, etc.

The controls shall include a joystick for PTZ camera control.

5.5.3.2 ***User Interface***

The IDAS shall provide SCC personnel with a full range of controls for managing, selecting, zooming and otherwise controlling all cameras, acknowledging alarms and acquiring data from the system.

The IDAS shall provide a map display for displaying the overall system. The map display shall permit the optional use of bilingual labels in Arabic and English. The display shall use color icons to annunciate perimeter status.

5.5.3.3 ***Displays***

The IDAS shall provide SCC personnel with multiple displays that allow easy visual monitoring of IDAS camera outputs.

The multiple display setup shall include, as a minimum, the following:

Display 1: Overview Map Display with all alarm location data.

Display 2: Split-screen display, preset or user selected, automatically switches to alarm zone display when alarm is triggered.

Display 3: Index Display for cycling through a random, or user selected, series of images from IDAS fixed and PTZ cameras. User shall have the choice to create an index of selected cameras that

are displayed simultaneously and updated at user selectable or preset intervals.

Display 4: PTZ camera display

All displays shall be minimum 1080p, or higher, capable displays sized 32" or larger. Displays shall be adequately sized to permit users to clearly see details.

5.5.3.4 ***Video Recording***

All images from Perimeter Surveillance & Perimeter Assessment cameras associated with an alarm and during an alarm event shall be recorded and retained for the intervals specified below before the data can be overwritten.

- Pre -Alarm recording: 5-20 seconds configurable
- Post-Alarm recording: 5-20 seconds configurable
- Perimeter Surveillance: 60 days
- Perimeter Assessment: 60 days

Alarm recording shall be at full HD 1080p resolution and 30fps.

The video shall be stored and available for viewing, locally and across the network.

5.5.4 **Performance Requirements**

5.5.4.1 ***Probability of Detection***

The IDAS system shall have a probability of detection capability of 95% that an intrusion attempt will be detected. This includes movement, cutting, climbing, lifting or digging, or any combination of these anywhere along the perimeter.

FO shall provide independent, third party evaluations & certifications, by internationally recognized institutions that verify compliance with this requirement.

5.5.4.2 ***Localization Accuracy***

The IDAS shall localize an alarm event within ±75 meters of where the intrusion occurs.

This localization may either be carried out in hardware or software.

Hardware Localization

Hardware localization is generally accomplished by limiting the size of detection zones and using its specific physical location as the localization parameter.

Software Localization

Software localization can be accomplished by using the geospatial coordinates of cameras, and the GIS display map, to localize an intrusion. This does require that the camera FOV be correlated to GIS coordinates so that the location can be accurately specified on a GIS map.

5.5.4.3 ***Nuisance Alarms***

Refers to an alarm generated by the sensor from a known cause that is not an intrusion attempt. Examples would be wildlife, blowing debris, or high wind speed triggering a sensor alarm. Sensors should be selected carefully so that they are suitable for the anticipated environmental conductions of the site to reduce the number of nuisance alarms generated.

The nuisance alarm rate is measured as total number of nuisance alarms may be averaged over the number of zones over a 30-day period.

This rate shall not exceed 1 alarm per zone averaged over the number of zones over a 30 day period.

5.5.4.4 ***False Alarms***

Refers to an alarm generated by the system for which there is no known cause. The alarms may be unknown due to assessment concerns (e.g. poor lighting or camera malfunction) or may be generated by the system. False alarms are often an indication that the system requires maintenance.

The total number of false alarms shall be averaged over the number of zones over a 30-day period and shall not exceed 1 false alarm per month maximum.

System Manufactures shall ensure the design features of IDAS control panels and their associated arming and disarming devices are

designed in accordance with ANSI/SIA CP-01-2014 to reduce the incidence of false alarm.

5.6 ID Management System

The IDentification card Management System (IDMS) shall manage, print, issue, and retrieve machine readable PIV cards for all personnel requiring access to company facilities.

The general requirements for the IDMS are as follows:

5.6.1 The IDMS shall produce, track and manage SEC-11 compliant PIV cards for issue to eligible personnel including both employees and contractors.

5.6.2 The IDMS shall consist of local IDMS workstations at a facility with a central IDMS server that shall store and retain all IDMS data online for at least 5 years.

5.6.3 All local IDMS workstation operations shall function with no loss of capability when communication links to the central IDMS are disrupted.

5.6.4 All card data shall be automatically replicated to the central IDMS at regular intervals of 10 minutes or less.

5.6.5 FO shall ensure that IDMS workstations are available in reasonable proximity to each facility using these PIV cards.

5.6.6 The IDMS shall provide data online to the ACS and other systems that use PIV cards.

5.6.7 PIV cards and PIV card management shall be fully compliant with the requirements of SEC-11.

5.7 Video Assessment & Surveillance System

The VASS provides surveillance capability for FO to monitor perimeters, gates, critical buildings and critical areas of the facility. The SRA shall designate the areas to be covered by the VASS.

5.7.1 **VASS Camera Performance**

5.7.1.1 VASS shall provide active surveillance capability under all weather conditions including low light, dense fog and sand storms.

5.7.1.2 Cameras that are used for surveillance and alarm generation must be fixed while assessment cameras shall use PTZ mounts to allow operators to move the camera and zoom in to the area of interest.

5.7.1.3 All VASS optical cameras shall be color cameras capable of low light operation. These shall be augmented by thermal cameras in selected locations to provide all weather capability.

5.7.2 **Geospatial Mapping Requirements**

5.7.2.1 All cameras shall be geospatially mapped to provide physical coordinates of each device.

5.7.2.2 FO shall use this capability to display imagery and alarm data on GIS maps that correlate each camera location to the map.

5.7.3 **VASS Imagery Processing**

5.7.3.1 All images from fixed cameras shall be processed by a Video Analytics System to facilitate the process of alarm detection and annunciation.

5.7.3.2 The video analytics system shall assist an operator in rapidly locating and determining the cause of sensor alarms by identifying activity in the camera scene where potential risk exists in the area being monitored.

5.7.3.3 The processing shall allow the detection of abnormal behavior such as, but not limited to, activity at a time when no activity is expected, packages left behind, entry into a restricted area or approach to a restricted area.

5.7.3.4 The VASS analyzing the video imagery shall have the ability for the operator to add new rules as required by local topography.

5.7.3.5 It shall have the ability to accept and integrate sensor inputs from other systems into its video processing algorithms.

5.7.4 **Camera Placement**

5.7.4.1 Cameras shall be placed based on local topography and applicable requirements.

5.7.4.2 The Operator shall carry out a study that defines the actual field of view of each camera/lens combination used and identifies blind spots. The study shall consider the actual focal length of the camera lens, camera pole height, local topography and obstructions in the camera field of view.

5.7.4.3 Camera coverage shall overlap so there are no blind spots between adjacent cameras.

5.7.4.4 ACS cameras shall allow clear views of the designated gate area.

5.7.4.5 Local terrain shall be used to determine the optimal camera mounting pole height that will meet the requirements of this Security Directive.

5.7.5 **Lighting**

Areas where cameras are deployed shall have lighting, fully compliant with SEC-04, to ensure optical cameras can display a clear image under all ambient lighting conditions.

5.7.6 **Long-Range Surveillance**

5.7.6.1 Long Range Surveillance (LRS) cameras shall have a range of 2km+.

5.7.6.2 Operator shall deploy LRS where required by SRA recommendations or HCIS. LRS may be required on the marine side of water facilities or at remote facilities.

5.7.6.3 LRS systems shall have the ability to monitor the area contiguous to the facility perimeter to evaluate situations as they are developing.

5.7.6.4 Facilities in open areas shall base the camera monitoring range on the time required to deploy a response to an alarm from the nearest security post. In no event shall this be less than 2 km.

5.7.6.5 Facilities shall use either radar (facilities in open areas only) or thermal sensors to detect activity in the monitored area under all conditions. These sensors, after their output has been processed, as specified in 5.7.3, shall be used by the system to automatically slew the LRS camera to the area of interest and annunciate an alarm.

5.7.6.6 Radar shall be optimized to detect personnel and vehicle sized targets. The radar beam shall automatically be blanked or turned off when the beam emission points towards the facility being protected.

5.7.6.7 This LRS shall be used to complement the IDAS which monitor actual intrusion attempts at or inside the perimeter.

5.7.7 **Video Recording**

All images from VASS cameras shall be recorded and retained for the intervals specified below, from the date the image was recorded, before the data can be overwritten. Recording shall be triggered by any motion in the camera field of view.

- Fixed Surveillance: 90 days
- Assessment: 30 days
- Alarm Events: 90 days

The video from all cameras shall be stored and available for viewing, locally and across the network.

5.8 Camera Specifications

All cameras shall comply with the following requirements:

5.8.1 **Image Quality**

5.8.1.1 All optical cameras shall operate at full High-Definition (HD) resolution of 1920x1080 pixels with progressive scan (1080p) at 30 frames/per second or higher.

5.8.1.2 Thermal cameras shall operate at 320x240 pixels, or higher, resolution in Long Wave Infra-Red (LWIR) at 30 frames/per second.

5.8.1.3 Cameras shall use automatic exposure control and be capable of outputting video at full frame rate or sub-multiples of the full frame rate.

5.8.1.4 Optical cameras may operate at fractional HD resolution and frame rate under normal conditions but must switch to full HD resolution and frame rate under alarm conditions.

The minimum resolution that can be used is 720p resolution at 7.5 frames per second.

5.8.2 **Focal Length & Zoom Capability**

All cameras shall have adequate focal length so that the operator can consistently distinguish between a human in any position or profile from an animal and debris anywhere in the covered zone.

نسخة مرخصة لشركة الدرع الوطنية

Assessment cameras shall have adequate zoom capability so that an operator can distinguish facial features of an intruder anywhere within the covered zone.

5.8.3 **Field of View**

5.8.3.1 The cameras field of view shall be adequate to cover the entire area under surveillance and be able to distinguish between a person and a nuisance alarm.

5.8.3.2 The smallest profile size of a human (i.e. standing, crouching, belly crawling, etc.) shall be discernible in all areas of the detection zone.

5.8.3.3 Clear zone width and length, cameras resolution and sensitivity, cameras location and smallest human profile shall all be considered when determining lens focal length.

5.8.3.4 All camera views shall overlap the views from adjacent camera in the detection zone so that there are no blind spots along the detection zone.

5.8.4 **Interface**

All cameras shall be able to connect directly to a LAN for transmission of imagery without any need for an external interface. LAN requirements are specified in SEC-08.

5.8.5 **Alarm Generation**

The system the camera is connected to shall annunciate an alarm when the video signal from a camera is lost.

5.8.6 **Camera Housing**

All camera shall have housings sealed to IP-66 or higher and shall meet the environmental constraints specified in SEC-01.

5.9 Plant Control Room

Plant Control Rooms present a special case for security compliance. The PCR may either be the main PCR for the facility or local PCR's designated critical by the FO. It shall be safeguarded against intruders and unauthorized visitors by the deployment of an ACS at the control room entrance door.

The ACS used at this facility shall be a scaled down version of the full ACS specified in this directive. It shall include at least two card readers on the entry side and a camera to permit plant control room personnel to observe personnel requesting

access. The ACS shall be powered by a UPS and access to a backup power generator when power to the ACS is interrupted.

5.10 Integration Requirements

All security systems shall be integrated into a common environment at the SCC. This section addresses requirements specifically for security systems.

5.10.1 The SCC shall present an integrated view to security personnel for all installed security systems. This does not preclude individual security system installation on physically discrete computers as technology limitations may preclude the optimal solution of a single, common hardware platform for all systems.

5.10.2 The SCC shall have the ability to present security personnel with a single interface and user environment for all installed security systems. This will allow security personnel to manage the systems from this environment without regard to the physical system distribution on different platforms.

5.10.3 Provision of this ability requires that all individual security systems transparently share data across secured links and permit the integration of security data with imagery from cameras and sensor activations.

5.10.4 This integrated environment shall be presented to security personnel across multiple displays that share common design and management techniques.

5.10.5 All ACS, ALPR, IDAS, IDMS, & VASS installations may continue to install specialized system monitoring equipment as dictated by individual system requirements.

5.11 Security Control Center

All security systems described above shall be integrated into a single command & control environment at the SCC. The SCC shall be tasked with managing and coordinating security assets and activities in a designated area.

5.11.1 The SCC design and layout shall comply with the requirements of ISO 110641-1 through 7.

5.11.2 The SCC shall be operated 24 hours a day, seven days a week, by trained operators who are familiar with the procedures, limitations and capabilities of managing the SCC.

5.11.3 The SCC integration platform software shall integrate the capability to manage ACS, ALPR, IDAS, IDMS, & VASS from the SCC console.

5.11.4 SCC operators shall have all SCC functions available to them in a single, multi-display console that integrates all security systems, communications

systems, surveillance, video and dispatch capability for mobile security assets. This shall allow the operator to manage and coordinate all security assets, in the area under his control, without having to access other systems.

5.11.5 The SCC operator shall manage and acknowledge all security system alarms, communicate with personnel via radio, hotlines or landlines, monitor gates and perimeter, view surveillance imagery from surveillance systems and dispatch security assets as needed, all from the single SCC console.

5.11.6 The SCC shall serve as a resource during activation of the facility Emergency Response Plan (ERP). The ERP is defined in SAF-20.

5.11.7 An ACS, with a video camera at the SCC door monitored inside the SCC, shall be used to manage access to the SCC.

5.11.8 Fire detection and fire protection systems, compliant with SAF-04, shall be installed in the SCC.

5.11.9 Computer installations in the SCC shall comply with the requirements of section 5.2 of this directive.

5.11.10 The SCC operator work area shall have no offices other than those required for SCC personnel.

5.11.11 The SCC shall have the ability to view and manage gates and facilities. Main gate cameras and crash barriers shall be monitored from the SCC. The ability to manage emergency activation and deactivation of the crash barriers from the SCC shall be provided.

5.11.12 The structure housing the SCC shall comply with the requirements of SEC-09.

5.11.13 All data required for the SCC function shall be provided to the operator at this console.

5.11.14 Personnel data and imagery shall be available to the SCC operator from the ACS.

5.11.15 All voice communications into and out of the SCC shall be recorded and maintained for 12 months.

5.11.16 Large Screen Displays shall be used to provide a continuous overview of the status of all areas under the SCC's control. Typically, this shall be accomplished using a video wall.

5.11.17 The SCC shall be powered by a dedicated UPS and emergency power generator as specified in SEC-07.

5.11.18 Security system components installed in the field shall have tamper sensors connected to the SCC that will annunciate an alarm when any attempt is made to access the component.

6 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
System Design Constraints	✓	✓	✓		
Access Control System	✓	✓	✓		
Automatic License Plate Recognition System	✓	✓	✓		
ID Management System	✓	✓	✓	✓	✓
Intrusion Detection & Assessment System	✓	✓			
Video Assessment & Surveillance System	✓	✓	✓	✓	
Camera Specifications	✓	✓	✓	✓	
Plant Control Room	✓	✓	✓		
Integration Requirements	✓	✓	✓		
Security Control Center	✓	✓	✓		

نسخة مرخصة لشركة المياه الوطنية

7 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-05 Reference	Requirement	FO Response
1.	5.2	System Design Constraints	*Submit system design document showing how each security system complies*
2.	5.3	ACS	*Submit system layout drawing, datasheets for main components and system design document showing technical details for each security system*
3.	5.4	ALPR	
4.	5.5	IDAS	
5.	5.6	IDMS	
6.	5.7	VASS	
7.	5.8	Camera Specifications	*Provide camera and housing specifications & datasheets*
8.	5.9	PCR	*Submit PCR ACS drawing and layout*
9.	5.10	Integration of Systems	*Submit details of integration platform, systems & functions that have been integrated, system layout drawing and a brief overview of how the system operates and interacts with the operator.*
10.	5.11	SCC	*SCC design specification documents & overview drawing showing layout.* *Submit evidence of ISO 110641-1 through 7 compliance*

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-06

Security Devices

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1. PURPOSE 7

2. SCOPE 7

3. ACRONYMS & DEFINITIONS 7

4. REFERENCES 8

5 GENERAL REQUIREMENTS 9

5.1 INSPECTION DEVICES 9

5.1.1. X-Ray System 9

5.1.2. Explosive Trace Detector 11

5.1.3. Metal Detection Archway 12

5.1.4. Under Vehicle Inspection System 12

5.2 PERSONNEL PROTECTION DEVICES 14

5.2.1. Ballistic Vest 14

5.2.2. Ballistic Protective Helmet 14

5.2.3. Ballistic Resistant Glass 15

5.3 BARRIER DETERRENCE 15

5.3.1. Raise Arm Barrier 15

5.3.2. Turnstile 16

5.3.3. Anti-Vehicle Barrier 18

6 APPLICATION OF REQUIREMENTS 22

7 PROOF OF COMPLIANCE (POC) 23

نسخة من خطة أمن شركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1. Purpose

This directive provides requirements for security devices installed at industrial facilities.

2. Scope

This Directive provides specifications, applicable certification standards and performance requirements for inspection devices, personnel protective equipment and barrier devices for gates and perimeters at facilities that are subject to the supervision of the High Commission for Industrial Security (HCIS), Ministry of Interior.

3. Acronyms & Definitions

ACS	Access Control System
AN	Ammonium Nitrate
ANFO	Ammonium Nitrate/Fuel Oil
AVB	Anti-Vehicle Barrier: There are three types of AVB: • Deployable AVB: *This type of AVB is deployed at gates in the vehicle traffic lanes & is commonly referred to as a* Road Blocker. • Fixed AVB: *This type of AVB is deployed as part of the perimeter fencing system.* • Bollards: *Bollards may be fixed or deployable. They are required for traffic management and roadway containment in the gate area.*
DMDNB	Dimethyl Dinitrobutane
DNT	Dinitrotoluene
EGDN	Ethylene Glycol DiNitrate or nitroglycol
ETD	Explosive Trace Detector
FO	Facility Operator – Owner, Operator or Lessee of a facility
HCIS	High Commission for Industrial Security.
HMTD	Hexamethylene Triperoxide Diamine
HMX	Octogen
HPU	Hydraulic Power Unit
NG	Nitroglycerine
PETN	PentaErythritol TetraNitrate or penthrite
RDX	Cyclotrimethylenetrinitramine: *aka* RDX, cyclonite, hexogen, T4
SCC	Security Control Center
SECNET	Security Network
Shall	Indicates a mandatory requirement.
Should	Indicates an advisory recommendation
SRA	Security Risk Assessment
TATP	Triacetone Triperoxide
TNT	Trinitrotoluene

نسخة من رخصة - هيئة الصناعة الوطنية

TSA	Transportation Security Agency, DHS
UVIS	Under Vehicle Inspection System

4. References

The current versions of the references in each SEC directive shall be applicable. They shall be considered integral to the SEC Directives.

ASTM A123	*Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products*
ASTM F2656-07	*Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*
ASTM F792-08$^{\varepsilon 2}$	*Standard practice for evaluating the imaging performance of security x-ray systems*
ISO/IWA 14-1:2013	*Vehicle Security Barriers. Performance Requirement, vehicle impact test method & performance rating*
NIJ 0101.06	*National Institute of Justice Standard 0101.06* *Ballistic Resistance of Body Armor*
NIJ 0108.01	*National Institute of Justice Standard 0108.01* *Ballistic Resistant Protective Materials*
NIJ 0601.02	*National Institute of Justice Standard 0601.02* *Walk-Through Metal Detectors for Use in Concealed Weapon and Contraband Detection*
PAS-68:2010	*BS PAS 68:2010, Specification for vehicle security barriers*
SEC-01	*Requirements for Security Directives*
SEC-07	*Power Supply*

5 General Requirements

FO shall deploy security devices needed for Inspection, Personal Protection and Barrier Deterrence.

5.1 Inspection Devices

Inspection devices shall be installed to detect any attempt to bring contraband into a protected facility through gates, pedestrian access and other entry points. These devices consist of, but are not limited to, X-Ray systems, Explosive Trace Detectors, Metal Detection Archways and Under Vehicle Inspection Systems.

5.1.1. **X-Ray System**

Certification

5.1.1.1. All X-Ray systems shall be certified by a credible government organization, such as TSA, or similar organization, to be used for inspection of personnel, packages and, where applicable, vehicles. The applicable certification shall be attached to all submissions of X-Ray system data sheets.

5.1.1.2. Each x-ray system shall have certification from a nationally recognized authority with regards to X-ray emission from the device after installation. This certification shall be renewed on an annual basis after a survey was conducted.

5.1.1.3. Each X-ray System shall have the certification level in the form of a tag or label permanently affixed to the device.

5.1.1.4. Each X-ray System shall have the name of the manufacturer, month and year of manufacture and place of manufacture in the form of a tag or label permanently affixed to the device.

Controls & Indicators

5.1.1.5. X-ray generation shall require the insertion of a key to grant permission to initiate the process. X-ray activation by any switch on the control panel, with the key removed, shall not be permitted.

5.1.1.6. The control panel shall have lights indicating unit status & X-ray emission.

5.1.1.7. Two independent means shall be provided to annunciate that the X-ray unit is emitting X-rays. Failure of a single component shall not cause failure of both annunciators.

نسخة من خصائص الهيئة العليا للأمن الصناعي

5.1.1.8. Clearly defined warning labels shall be affixed to the unit bearing the statement "CAUTION: X-RAYS PRODUCED WHEN ENERGIZED" shall be affixed in a clearly visible position. This warning shall be listed in Arabic & English.

5.1.1.9. The control panel shall include an emergency switch to terminate X-ray generation.

Safety Features

5.1.1.10. Radiation emitted from the X-ray unit cabinet shall not exceed 0.5 milliroentgen in one hour at any point five centimeters outside the cabinet.

5.1.1.11. The insertion of any part of the human body through any port into the primary beam shall not be possible.

5.1.1.12. Each door of the X-ray unit shall have at least two safety interlocks. At least one of these interlocks shall cause the physical disconnection of the energy supply circuit to the high voltage generator.

5.1.1.13. Each access panel shall have at least one safety interlock.

5.1.1.14. Failure of any single component in the X-ray unit shall not cause failure of more than one required safety interlock.

5.1.1.15. A ground fault shall not result in the generation of X-rays.

Operation

5.1.1.16. Personnel operating the unit shall work for a maximum of 90 minutes. They shall then work on other activities for at least 90 minutes prior to being reassigned this task.

5.1.1.17. This measure shall be put in place to ensure that the operator is fully concentrated on his task. The skill level and focus of the operator are the key elements in correct interpretation of the image.

5.1.2. **Explosive Trace Detector**

FO shall deploy explosive detection capability at facility gates by using mobile or desktop units optionally complemented by K9 units. Mobile or Desktop Explosive Trace Detectors (ETD) shall incorporate the requirements of this section.

5.1.2.1. While these specifications are specifically for ETD's they do not remove the need for the FO to evaluate related operational issues of deploying additional devices such as K9, X-ray units and metal detectors that can improve the effectiveness of ETD's.

5.1.2.2. All ETD's shall be constructed of materials and components that will permit extended, continuous operation under the environmental conditions listed in SEC-01.

5.1.2.3. ETD's shall be certified, by independent, internationally recognized authorities, that the device meets the specifications as published by the manufacturer for the specific device.

5.1.2.4. Explosives Detected: TNT, RDX, PETN, NG, EGDN, DNT, AN, ANFO, HMTD, HMX, TATP, double base smokeless & black powders, Tetryl, Picric Acid, Nitrated explosives & common taggants such as DMDNB & mononitrotoluenes. Vendor shall notify FO of explosives that cannot be detected.

5.1.2.5. The ETD shall be capable of detecting all explosives with swipe, vapor detection or both, depending on facility operational requirements.

5.1.2.6. Detection Limits: 1 microgram of each target.

5.1.2.7. Alarm Annunciation: Audio & Visible alarm with a clear display of the explosive type detected.

5.1.3. **Metal Detection Archway**

Metal Detection Archways shall be installed at facilities to detect any metal objects carried by personnel entering the facility.

5.1.3.1 Archways shall comply with all standards for metal detection archways listed under National Institute of Justice Standards 0601.02.

5.1.3.2 The supplier shall provide verifiable certification for compliance with this standard.

5.1.3.3 FO shall implement pedestrian traffic flow management to ensure that the archway cannot be bypassed.

5.1.3.4 Where security operations dictates, certified hand wands may be utilized.

5.1.4. **Under Vehicle Inspection System**

Under Vehicle Inspection Systems (UVIS) shall be deployed to view and evaluate vehicle undercarriages which are traversing main gates leading into designated facilities.

5.1.4.1 UVIS systems shall be deployed in all entry lanes at all gates providing access into the following facilities:

a. Industrial Cities
b. Sea Ports
c. Class 1 facilities
d. Where required by an SRA

5.1.4.2 The UVIS system shall incorporate the following:

a. UVIS shall be mounted in a vertical deflection device, such as a speed hump, to reduce vehicle speeds as they transit the UVIS camera.
   The UVIS mounting shall be rated for the maximum weight of vehicle expected to transit the device.
b. UVIS shall incorporate both optical and infra-red to illuminate the vehicle undercarriage while acquiring the image.
c. The UVIS undercarriage camera shall have Full High Definition (HD) or fractional HD (720p) resolution at a minimum.

نسخة مرخصة لشركة لينا الوطنية

d. UVIS imagery shall be retained and correlated to the license plate number of the vehicle crossing the UVIS[1].

e. UVIS imagery shall be compared against previous[2] entries by the vehicle. Any variations shall be automatically highlighted and displayed to security personnel for further action.

f. UVIS shall automatically compensate for vehicle undercarriage height variations between passenger vehicles and large trucks when taking undercarriage images.

5.1.4.3 UVIS imagery shall be retained as needed to ensure vehicle imagery used for comparison is available even for vehicles with infrequent entries to the facility.

5.1.4.4 FO shall ensure that the UVIS is located so that there is adequate time for UVIS image acquisition, evaluation and alarm annunciation prior to vehicle reaching gate security personnel.

5.1.4.5 UVIS shall be constructed of materials and components that will permit extended, continuous operation under the environmental conditions listed in SEC-01.

نسخة من دليل شركة المياه الوطنية

[1] *FO may use a separate UVIS specific license plate camera or interface with the Automatic License Plate Recognition System (ALPRS) specified in SEC-05, section 5.4 to acquire license plate data. In all cases license plate data shall be acquired automatically with no operator intervention.*

[2] *If no previous record exists for a vehicle license plate, UVIS shall alert security personnel to take steps to register vehicle details in the appropriate system.*

5.2 Personnel Protection Devices

FO shall provide ballistic vests, ballistic protective helmets and ballistic resistant glass to protect all security personnel working at gates. Procedures shall be developed by the FO to define the use and conditions under which they must be worn by security personnel at the gates.

5.2.1. **Ballistic Vest**

5.2.1.1 Ballistic Vest shall be provided to security personnel for personal protection.

5.2.1.2 Ballistic vests provided for Security Directive compliance shall comply with the performance standards for Type III armor listed under NIJ 0101.06.

5.2.1.3 All Ballistic Vests & Ballistic Panels shall have clearly affixed labels citing standards compliance in accordance with NIJ 0101.06.

5.2.1.4 FO shall replace any ballistic vest that, during its life cycle, develops wrinkles, blisters, cracks or fabric tears, crazing, chipped or sharp corners and edges, or other evidence of inferior workmanship.

5.2.1.5 Ballistic vests shall be certified, by independent, internationally recognized authorities, that the device meets the applicable NIJ standards.

5.2.2. **Ballistic Protective Helmet**

5.2.2.1. Ballistic protective helmets shall be provided to security personnel for personal protection.

5.2.2.2. Ballistic protective helmets provided for Security Directive compliance shall comply with the performance standards for Type III armor listed under NIJ 0101.06.

5.2.2.3. Ballistic protective helmets shall be certified, by independent, internationally recognized authorities, that the device meets the applicable NIJ standards.

5.2.3. **Ballistic Resistant Glass**

5.2.3.1. Ballistic resistant glass and frames shall be installed in gatehouses and other security facilities requiring ballistic protection. Document pass through windows in these facilities shall comply with the standards of this security directive.

5.2.3.2. Ballistic resistant glass shall be capable of meeting the requirements of NIJ 0108.01 and shall provide protection against Type III ammunition as defined in this NIJ standard.

5.2.3.3. The frame in which the ballistic resistant glass is installed shall be certified to the same level as the glass itself.

5.2.3.4. Ballistic resistant glass, and frames, shall be certified, by independent, internationally recognized authorities, that the material and design meets the applicable NIJ standards.

5.3 Barrier Deterrence

FO shall deploy raise arm barriers and turnstiles at gates to manage vehicular and pedestrian traffic and provide certified Anti-Vehicle Barriers (AVB) at perimeters, main gates, process area gates and entrances to critical facilities.

5.3.1. **Raise Arm Barrier**

Raise arm barriers provide administrative barriers for managing vehicle traffic flow into secured facilities.

5.3.1.1 All raise arm barriers shall be constructed of materials and components that will permit extended, continuous operation under the environmental conditions listed in SEC-01.

5.3.1.2 The barriers shall be system operated when installed for Security Directive compliance.

5.3.1.3 The barrier housing shall be manufactured of stainless steel, hot-dipped galvanized steel, powder coated steel or aluminum painted in high visibility colors. Access to the housing shall be via an adequately sized door that permits maintenance personnel to remove and replace any component.

5.3.1.4 The housing shall incorporate a single, two position, externally mounted switch that permits the barrier boom to be either manually raised or lowered and placed under system control.

5.3.1.5 The device shall have the ability to function completely under the control of an external access control system.

5.3.1.6 If boom encounters an obstruction it shall immediately change direction and return to the raised or lowered position.

5.3.1.7 If boom is hit by a vehicle, it shall break or disengage from its mounting. It shall also incorporate a sensor such that if the boom is broken it shall activate the crash barrier(s) and annunciate an alarm to the SCC and the local gatehouse.

5.3.1.8 The boom shall span the entire traffic lane. It shall be painted in high visibility, fluorescent colors.

5.3.2. **Turnstile**

5.3.2.1. Turnstiles shall be operated by the ACS when installed for Security Directive compliance.

5.3.2.2. Vehicle barriers (such as bollards or other style vehicle barrier devices) shall be installed in front of turnstiles to prevent vehicles from entering the turnstile areas.

5.3.2.3. Turnstiles installed for Security Directive compliance shall comply with the following requirements:

Structural		
1.	Main Body	Stainless steel, hot-dipped galvanized steel, powder coated steel or anodized aluminum.
2.	Arms	Stainless steel, minimum schedule 40 pipe, minimum diameter of 3.8cm (1.5inch) with maximum centerline spacing of 20cm (8 inch).
3.	Configuration	Four fixed arms at 90 degrees to each other, arms shall pass between adjacent fixed arms secured to the body of the turnstile.
4.	Bottom Assembly	The bottom of the main turnstile column shall use a dust and water proof thrust bearing.
5.	Top Assembly	Easy accessibility for maintenance personnel from inside the facility.
6.	Cabling	All cabling to the turnstile shall be via steel flexible conduit or steel conduits as acceptable under local electrical codes.

نسخة من الشركة المياه الوطنية

7.	Installation	Turnstile shall be secured top and bottom to a rigid structure. All areas around the turnstiles (above, between, beside) shall be secured with anti-personnel security features to prevent personnel from bypassing the turnstiles.

Controls

8.	Manual Override	Turnstile shall have a mechanical manual override key-switch for each turnstile. Key-switch shall be switchable for entry, exit or free rotation. Positive key control shall be maintained. Status of this switch shall be annunciated to the ACS.

Performance

9.	ACS Control	ACS shall control locking & unlocking of device.
10.	Failure Modes	Entry: Fail-Lock when power is lost. Exit: Fail-Open when power is lost.
11.	Rotation Sensor	Sensor shall detect rotation and notify ACS when device is rotated
12.	User Sensor	Pressure plate in turnstile base OR optical sensor at turnstile egress OR other sensor to positively confirm that user has actually passed through the turnstile AFTER an ACS approved access request. Sensor shall annunciate event to an external system. ACS shall log user in OR out based on this positive verification of user transit through the device.
13.	Auto-Lock	Turnstile shall auto-lock, at 90 degree position, after access is granted if the turnstile is rotated or shunt-time is exceeded.
14.	Component Rating	All components shall have adequate power ratings to guarantee 24 hour / 7 day a week / 365 days a year operation under the environmental requirements stated in SEC-01.
15.	Power Supply	Power supplied to this device shall be backed up by an emergency generator and shall fully comply with the requirements of SEC-07. Each turnstile shall be powered by an individual circuit breaker.

نسخة غير خاصة لشركة المياه الوطنية

5.3.3. Anti-Vehicle Barrier

Anti-Vehicle Barriers (AVB) provide certified solutions to prevent the ingress of vehicles into a facility. HCIS shall not consider AVB's without required certification.

AVB's generally consist of 3 separate types:

- Road Blocker: Deployable AVB installed in exit and entry lanes of facility gates. The minimum deployed road blocker height shall be 90cms.
- Anti-Vehicle Fence: Fixed AVB installed along facility perimeter as part of the fencing system at a Class 1 facility.
- Bollard: Fixed or deployable AVB installed along roadways or in front of structures to prevent vehicle ingress into those areas.

AVB's shall be installed in all areas designated below:

- Exit and entry lanes at Class 1 through 4 Main Gates
- Class 1 through 3 Process Area Gates
- Entire Class 1 perimeter fence
- At Emergency gates at Class 1 & 2 facilities

In all cases, AVB's deployed at industrial facilities shall comply with the following requirements:

5.3.3.1 AVB shall be rated M50-P1 as defined in ASTM F2656-07. This rating limits penetration of the vehicle to 1m under specified test conditions.

FO may alternatively use PAS-68 or ISO/IWA 14-1 as long as they are rated equivalent to the ASTM rating of M50-P1. FO shall present documentation from the AVB manufacturer to support this equivalence.

In all cases FO shall submit certificates from an accredited test agency to validate the rating. The certificate must state that the AVB was successfully impact tested to the submitted rating level.

FO may use lower rated bollards for gate traffic management when permitted by gate design and with adequate justification.

5.3.3.2 Lower rated ASTM F2656-07 certified barriers may be used if terrain characteristics tangibly limits acceleration or top speed potential in a designated area of the perimeter and there is no impact on the facility from the extended penetration rating.

FO shall provide HCIS with justification why the lower rated barriers are acceptable due to limited vectors for acceleration, access and/or due to other reasons. The reasons cited for this use shall be valid for all approaches to the facility perimeter where the barrier is installed. The use of such lower rated barriers shall be concurred by HCIS prior to their incorporation in the design and implementation.

This justification shall be provided in a formal engineering study that justifies the use of the lower rated barrier.

5.3.3.3 The AVB manufacturer shall provide AVB installation methodology showing the precise method for AVB installation based on an analysis of local soil conditions. FO shall secure certification from the manufacturer that the installation methodology shall continue to provide the level of protection specified in the ASTM F2656-07 rating.

This shall be similar to the methods used for securing the AVB for certification tests. The installation shall include facilities for drainage and required maintenance procedures.

5.3.3.4 All AVBs shall be constructed of materials and components that will permit extended, continuous operation under the environmental conditions listed in SEC-01.

5.3.3.5 All steel components and fasteners shall be protected against corrosion by hot-dip galvanizing in compliance with ASTM A123 or an acceptable equivalent corrosion protection standard.

5.3.3.6 Deployable road blocker installations shall comply with the following requirements:

5.3.3.6.1. All AVBs shall have traffic light type indicators either adjacent to each AVB or above the lane in which the AVB is installed.

5.3.3.6.2. The traffic lights shall have independent lights AVB lowered (amber or green) and AVB deployed (red color). The lights shall change state automatically depending on AVB position.

5.3.3.6.3. In deployed position the AVB shall have painted markings, in high-visibility fluorescent colored stripes, facing oncoming vehicles, to advise them that the AVB is deployed.

5.3.3.6.4. The AVB shall be controlled by a control panel inside the gatehouse with normal deploy and retract switches. The control panel shall have status lights indicating AVB deployment.

5.3.3.6.5. The control panel shall include an emergency deployment switch. The switch shall have a protective mechanism to prevent accidental activation but shall permit easy activation when required.

Activation of the emergency switch shall raise all AVBs at the gate. The normal deploy/retract buttons shall not affect AVB operation once the emergency deploy button has been activated.

Retraction of the AVB after emergency deploy shall require activation of a key-switch or a command from a remote SCC to retract the AVB. A single key-switch shall control multiple AVBs for clearing the emergency deployment switch activation.

Once the emergency switch has been re-set the normal deploy/retract switches shall be reactivated.

5.3.3.6.6. The AVB shall incorporate active sensors and safety features that will prevent normal AVB deployment if there is a vehicle obstructing its deployment path. These safety features shall not affect emergency deployment.

5.3.3.6.7. Normal operation deploy/retract: 3 - 5 seconds max
Emergency Deploy: less than 1.5 seconds

5.3.3.6.8. The AVB shall be operated using hydraulic or electromechanically powered mechanisms.

Hydraulic Power Units (HPU) shall be adjacent to, or within 10m, of the actual AVB installation and located within the facility perimeter. Each HPU shall power only one AVB.

Any HPU shall be designed to allow at least 3 - 5 complete deploy/retract cycles if power to the HPU is interrupted.

The AVB shall Fail Secure. For any AVB gates utilizing hydraulic systems that do not have fail secure features installed, the FO shall provide ballistic protection to both the HPU and any hydraulic line junction boxes.

5.3.3.6.9. The AVB shall have the ability to interface with external computer systems as listed below:

- Remote control and integration with the facility ACS.
- Connect to the SCC.
- SCC shall have the ability to operate the AVB and execute emergency deployment & retraction.
- FO shall provide clearly documented procedure, protocols and formats for AVB connectivity to an external system or location across the SECNET data network. The level of detail provided shall be adequate to permit FO to develop the relevant control software on an external computer system.

5.3.3.6.10. When in retracted position AVBs installed in roadways shall be rated to handle the weight of vehicles passing over them with no impact on performance.

Wheel load limits based on the heaviest loaded vehicles for each site will be determined and used in specifying the AVBs for that site.

نسخة من الهيئة العليا للأمن الصناعي

6 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on its FSC. FO may use SRA recommendations, with valid justification, to amend the application of the requirements specified below:

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
X-Ray Systems	✓	✓	✓		
Explosive Trace Detector	✓	✓	✓		
Metal Detection Archways	✓	✓	✓		
Under Vehicle Inspection System	✓				
Ballistic Vest	✓	✓	✓		
Ballistic Protective Helmets	✓	✓	✓		
Ballistic Protective Glass	✓	✓	✓	✓	✓
Raise Arm Barriers	✓	✓	✓	✓	✓
Turnstiles	✓	✓	✓	✓	
Anti-Vehicle Barrier	✓	✓	✓	✓	

نسخة من شركة المياه الوطنية

7 Proof of Compliance (PoC)

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items. The Stage 3 submission, content and format are specified in SEC-14 section 6.3. This PoC shall form part of Section 3 of the Stage 3 submission package.

This PoC shall provide details for each of the requirements listed below.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-06 Reference	Requirement	FO Response
1.	5.1.1	X-Ray Certification	*Attach certified x-ray list from accreditation agency & technical brochure for device*
2.	5.1.2	ETD Certification	*Attach certified ETD list from accreditation agency & technical brochure for device*
3.	05.1.3	MDA Certification	*Attach certified MDA list from accreditation agency & technical brochure for device*
4.	5.1.4	UVIS Data	*Submit manufacturer technical brochure & responses to all items in section 5.1.4.*
5.	5.2.1.1 - 5	Ballistic Vest	*NIJ Compliance certification data*
6.	5.2.2.1 - 3	Ballistic Helmet	*NIJ Compliance certification data*
7.	5.2.3.1 - 4	Ballistic Glass	*NIJ Compliance certification data*
8.	5.3.1.	Raise Arm Barriers	*Submit manufacturer technical brochure*
9.	5.3.2.	Turnstile	*Submit manufacturer technical brochure & responses to 5.3.2.3-9 through 15*
10.	5.3.3.	AVB	*Certification specified in 5.3.3.3* *Manufacturer installation certification as specified in 5.3.3.5* *Responses to 5.3.3* *Manufacturer technical brochure*

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-07

Power Supply

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7

2 SCOPE 7

3 ACRONYMS & DEFINITIONS 7

4 REFERENCES 7

5 GENERAL REQUIREMENTS 8

5.1 INCOMING UTILITY POWER 8
5.1.1. Main Utility Power Feed 8
5.1.2. Alternate Utility Power Feed 8
5.1.3. Automatic Utility Power Feed Switching 8
5.1.4. Power Conditioning & Lightning Protection 9
5.2 EMERGENCY POWER GENERATOR 9
5.3 UNINTERRUPTIBLE POWER SUPPLY (UPS) 11
5.4 GROUNDING 12
5.5 SUPPORT & MAINTENANCE 12

6 APPLICATION OF REQUIREMENTS 13

7 PROOF OF COMPLIANCE 13

8 APPENDIX A: TYPICAL SINGLE LINE DIAGRAM ..... ERROR! BOOKMARK NOT DEFINED.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document provides requirements for power supply to security systems at industrial facilities.

2 Scope

This Directive provides the minimum requirements for companies and establishments that are subject to the supervision of the High Commission for Industrial Security (HCIS), Ministry of Interior, for power supply to security systems at industrial facilities.

3 Acronyms & Definitions

FO	Facility Operator: the owner, operator or lessee of a facility
HCIS	High Commission for Industrial Security
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
UPS	Uninterruptible Power Supply

4 References

This directive adopts the latest edition of the references listed.

The selection of material and equipment, and the design, construction, maintenance, operation and repair of equipment and facilities covered by this Security Directive shall comply with the latest edition of the references listed in each Security Directive, unless otherwise noted.

IEC 62040	*Uninterruptible power systems (UPS) - Part 1: General and safety requirements for UPS*
IEEE 519	*Recommended Practice & Requirements for Harmonic Control in Electric Power Systems*
IEEE C62.41.1991	*Practice for Surge Voltages in Low Voltage AC Power Circuits*
NFPA 110	*Standard for emergency and standby power systems.* *NFPA 110 figure A.8.3.1 (a). Emergency Power Supply maintenance and tests.*
NFPA 780	*Standard for installation of lightning protection systems.*
SEC-01	*General Requirements for Security Directives*
SEC-05	*Security Systems at Industrial Facilities*
SEC-15	*Security Management at Industrial Facilities*

5 General Requirements

Power supply to all security facilities, systems, networks, devices and infrastructure shall consist of a combination of main AC power from a reliable public utility source, an alternative power source, on site dedicated backup sources, automatic switching between main and backup power sources and full protection against sags and surges in the incoming power.

See attached typical single line diagram in Appendix A.

5.1 Incoming Utility Power

5.1.1. **Main Utility Power Feed**

The main power supply feed that supplies the security systems at the facility shall be sourced from facility essential switchgear (where available), adequately sized, and installed, to meet all requirements for operation of all security systems and components.

5.1.2. **Alternate Utility Power Feed**

The alternate power supply shall feed the security systems at the facility in case of main utility power feed failure.

5.1.3. **Automatic Utility Power Feed Switching**

5.1.3.1. The facility shall have dedicated transfer switchgear (ATS with 1 second time delay) that will execute an automatic, unattended changeover between main and alternate power feeds as needed.

5.1.3.2. In case of failure of both main and alternate utility power feeds, the emergency power generator shall execute an automatic start, with a 5 second time delay (to compensate for transient under voltage conditions) and supply power within 30 seconds of the power interruption.

5.1.3.3. A power failure is defined as a voltage excursion greater than -20%/+10% of nominal.

5.1.3.4. There shall be an interlock between emergency power generator breakers and the automatic transfer switchgear.

5.1.3.5. Failure of the power supplied to any security related systems or components shall be sensed and annunciated at the gate house and at the SCC specified in SEC-05.

نسخة من دليل شركة المياه الوطنية

5.1.3.6. System shall automatically revert to the main feed upon its restoration with no manual intervention required.

5.1.3.7. In case of total failure of the electric power system including the UPS and disruption of system operation, the system shall restart automatically, upon resumption of the electrical power, to all previous settings that were used before the disruption of the utility power feed.

5.1.4. **Power Conditioning & Lightning Protection**

5.1.4.1. All incoming power shall be conditioned and protected against surges, sags and harmonic variation by the deployment of surge suppressors and appropriate voltage correction devices as mandated by IEEE 519 and IEEE C62.41.1991.

5.1.4.2. The wiring shall incorporate protection against lightning strikes as mandated by NFPA 780.

5.1.4.3. The circuit breakers for both the primary and alternate AC sources shall be equipped with overcurrent protection, sized and coordinated with upstream and downstream protection.

5.2 <u>Emergency Power Generator</u>

All facilities that deploy security systems for Security Directive compliance shall have emergency power generators installed.

5.2.1 FO shall install emergency power generators that exclusively power all security infrastructure, systems and devices at facilities.

5.2.2 The generator shall be sized to power all security systems & devices, air conditioning, lighting, fence lighting and communications equipment installed at the security facility while maintaining at least 20% spare capacity.

5.2.3 The generator can be installed locally, at the facility, or at a remote location. In all cases it shall be located within a secured facility perimeter fence.

5.2.4 Regardless of the location of the generator:

5.2.4.1 It shall be installed in an enclosure, or building, that protects it from the environment and prevents unauthorized ingress to the generator and its controls.

5.2.4.2 It shall be able to sense power failure at the incoming local utility power feed to the security system, as referenced in 5.1.3.2, and initiate startup to supply power.

5.2.5 The generator shall have dedicated automatic startup capability that will execute an automatic, unattended generator start and change over to the generator within 30 seconds of the failure of the main local utility power feed with no manual intervention required.

The 30 seconds includes the time allowed for the generator to start, the output to stabilize and it begins supplying power to the load.

System shall automatically revert to the main utility power feed upon its restoration with no manual intervention required. A manual bypass capability shall also be provided inside the generator housing.

5.2.6 The fuel tank for the generator shall have a low level alarm when the fuel level drops to 10% of full capacity. The alarm shall be activated in the guardhouse and SCC to inform security personnel and SCC operators.

5.2.7 The generator shall have as a minimum, a fuel tank sized for continuous 24 hours operation at full load.

5.2.8 The structure housing the emergency generator shall not be part of the perimeter fence and shall be located at least 50m away from the fence.

5.2.9 Generators installed near the facility shall have acoustic barriers rated to reduce the noise to an acceptable level at the nearest occupied offices.

5.2.10 The exhaust pipes from each generator shall be fitted with a spark arrestor and shall terminate above the roof of the housing.

5.2.11 When a generator and automatic transfer switch arrangement is used to extend the protection time of a UPS system, it shall be connected to deliver power to the UPS rectifier, but not directly to the critical load.

5.3 Uninterruptible Power Supply (UPS)

All facilities that deploy security systems for Security Directive compliance shall have dedicated UPS's installed.

5.3.1 The UPS shall be dedicated to powering security system components and facilities.

5.3.2 The UPS shall be sized to power all security systems, network interface, displays, printers and workstations.

The UPS shall not power single entry devices, such as drop gates and turnstiles, lighting or air conditioning.

5.3.3 The UPS shall be capable of accepting two incoming power circuits and using either one of them to power the UPS.

It shall incorporate an internal static switch for changeover between incoming power and batteries and a manual bypass switch to allow maintenance of the system.

5.3.4 The UPS shall have installed battery capacity to power its maximum rating for 2 hours minimum. The UPS shall be sized with 30% spare capacity over and above the actual calculated load.

All batteries shall be specifically designed for use in UPS systems and certified by the manufacturer for such use. The use of vehicle batteries is specifically prohibited.

5.3.5 Internal UPS faults shall be annunciated in the gate house and security control center, by a remotely mounted panel and shall also be included in security system logs.

5.3.6 UPS shall automatically initiate a security system computer shutdown (to protect the computers) if UPS battery levels drop below the level required to power the security system during a power outage.

5.3.7 The UPS shall be located adjacent to the security computer system in a separate room.

5.3.8 The UPS room shall be air conditioned to the same requirements as the security system.

5.4 Grounding

5.4.1 All security facilities, systems, networks, devices and infrastructure shall be properly grounded in accordance with this directives.

5.4.2 All power systems that supply power to security systems or components shall ensure that the power system is properly grounded to maximize performance, reliability and safety.

5.4.3 The grounding system shall be designed and constructed in accordance with NFPA 70, article 250.

5.5 Support & Maintenance

All electrical components deployed for compliance with this directive shall be tested and maintained in accordance with applicable requirements in SEC-15.

نسخة مرخصة لشركة المياه الوطنية

6 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on its FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Primary Utility Power Feed	✓	✓	✓	✓	✓
Alternate Utility Power Feed	✓	✓	✓	✓	
Automatic Utility Power Feed Switching	✓	✓	✓		
Power Conditioning & Lightning Protection	✓	✓	✓	✓	✓
Emergency Power Generators	✓	✓	✓		
Uninterruptible Power Supply	✓	✓	✓		
Grounding	✓	✓	✓		
Support*	✓	✓	✓		

7 Proof of Compliance

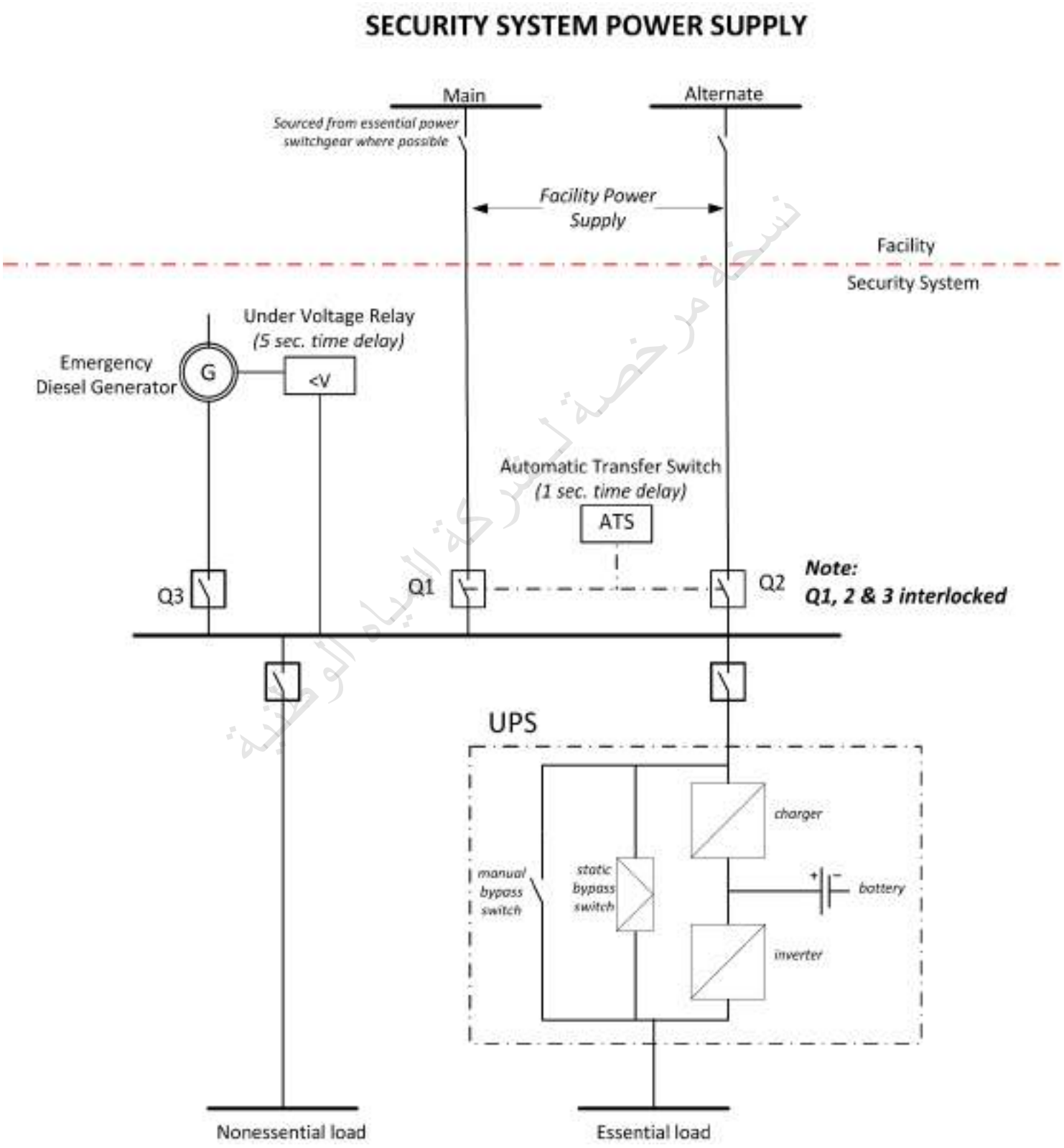
FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 1 or Stage 3 workflow (as specified), to demonstrate how the FO is complying with specific requirements in this directive.

This PoC shall provide the details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-07 Reference	Requirement	FO Response
1.	5.1.3	Automatic switching	*Provide automatic switch overview and single line diagram*
2.	5.1.4	Power conditioning	*Provide power conditioning and lightning protection overview and single line diagram*
3.	5.2	Generator	*Submit datasheets & compliance list for generator*
4.	5.3	UPS	*Submit datasheets & compliance list for UPS*
5.	5.4	Grounding	*Provide grounding overview and single line diagram* *List actual neutral to ground voltage measurements in gatehouse and support building receptacles where security systems are connected*

8 APPENDIX A: Typical Single Line Diagram



نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-08

Security Communications & Data Networks

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7

2 SCOPE 7

3 ACRONYMS & DEFINITIONS 7

4 REFERENCES 8

5 GENERAL REQUIREMENTS 9

5.1 WIRED COMMUNICATIONS 9
5.2 WIRELESS COMMUNICATIONS 11
5.3 POWER SUPPLY 15
5.4 MAINTENANCE & SUPPORT 15
5.5 SECURITY 15

6 APPLICATION OF REQUIREMENTS 16

7 PROOF OF COMPLIANCE 17

APPENDIX A: SECNET OVERVIEW DIAGRAM 18

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document provides requirements for implementing secured communication services for industrial security and emergency response at industrial facilities.

2 Scope

This directive provides FO with the requirements for secure and encrypted, wired and wireless communications and data networks utilized for security, firefighting and emergency response services at facilities under the jurisdiction of the HCIS.

3 Acronyms & Definitions

AVL	Automatic Vehicle Location
CITC	Communications & Information Technology Commission
FO	Facility Operator: the owner, operator or lessee of a facility
GIS	Geographic Information System
HCIS	High Commission for Industrial Security
IEC	International Electro-Technical Commission
LAN	Local Area Network
MDM	Mobile Device Management
PIC	Preliminary Inspection Point
SCC	Security Control Centers
SECNET	Security Network
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
SSL	Secure Sockets Layer
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point

4 References

This directive adopts the latest edition of the references listed.

The selection of material and equipment, and the design, construction, maintenance, operation and repair of equipment and facilities covered by this Security Directive shall comply with the latest edition of the references listed in each Security Directive, unless otherwise noted.

ANSI/TIA-222-G	*Structural Standard for Antenna Supporting, Structures and Antennas*
ANSI/TIA-568-A	*Telecommunications Cabling Standards for Voice, Video and Data Networks*
ANSI/TIA-758-A	*Customer Owned Outside-Plant Telecommunications*
AES 256	*Advanced Encryption Standard*
CAT 6	*Category 6; standardized twisted pair cable for gigabit Ethernet*
IEC 60086	*Environmental Testing*
IEC 60255	*Electrical Relays-International Electro-Technical Commission*
IEC 60529	*Degrees of Protection Provided By Enclosures (IP Code)*
IEC62040	*Uninterruptible Power Systems (UPS)*
IEC 62305	*Protection Against Lightning*
NFPA 70	*National Fire Protection Association: National Electric Code*
SEC-01	*General Requirements for Industrial Security*
SEC-02	*Security Fencing*
SEC-05	*Security Systems at Industrial Facilities*
SEC-07	*Power Supplies*
SEC-09	*Structures Housing Security Equipment*
SEC-12	*Information Protection & Cyber Security*
SAF-12	*Electrical Safety*
SEC-15	*Security Operations at Industrial Facilities*

5 General Requirements

Communications and networks for security systems deployed for SEC & SAF compliance shall use both wired and wireless technologies for the transfer of voice, data and video related to security, safety and fire protection services at a facility.

5.1 Wired Communications

5.1.2 Voice

FO shall provide a hotline, *i.e.* a direct telephone line in constant operational readiness so as to facilitate immediate communication between each gate & its PIC, onsite government forces & the facility SCC.

FO may deploy additional hotlines as needed based on an internal assessment of requirements.

Adequate standard phone lines shall be available at each security facility to manage administrative requirements.

5.1.3 Data

5.1.3.1 Wired communications infrastructure installed for compliance with this Security Directive shall use fiber optic cable.

- All cabling and equipment shall comply with requirements stated in TIA-568-A or TIA-758-A.
- All maintenance holes shall be locked.
- All cabinets, cable shields and equipment installed for security applications shall be grounded in accordance with the provisions of NFPA 70 and prevailing telecommunications standards.
- Cables that are above ground shall be placed in steel conduit.
- All junction boxes shall use tamperproof fasteners.
- The system shall have mechanisms in place to detect any attempt at tampering with the cabling and devices.

5.1.3.2 The LAN deployed at each security facility shall be dedicated to security systems and designated as SECNET.

- SECNET shall be implemented with redundant, physically discrete networks.
- SECNET cabling shall be physically installed in separate discrete physical ducts or sub-ducts, i.e., it shall use route diversity, from the security facility to the central facility.
- All SECNET LAN cabling shall comply with CAT-6 requirements with all connectors and cabling rated for minimum 1000BaseT (Gigabit Ethernet) speeds.
- All security devices with LAN connectivity requirements shall have two, physically discrete, network connections and shall automatically connect to the active LAN.
- SECNET shall have a dedicated router/switch to connect to a backbone or public network.

Attached see Appendix A for an overview of SECNET topology.

5.1.3.3 Where SECNET connects to a backbone or public network it shall be protected with a Firewall appliance, consisting of hardware and software that controls incoming and outgoing network traffic into SECNET based on rules that limit access exclusively to authorized security systems and users. FO shall ensure that the firewall is properly configured to manage SECNET access.

5.1.3.4 SECNET shall deploy Intrusion Detection & Prevention appliances to detect any attempt to intrude into SECNET and/or its devices.

5.1.3.5 SECNET shall operate at a minimum of 1000baseT (Gigabit Ethernet). All devices connected to SECNET shall have native 1000BaseT network connection speeds. All switches and routers used on SECNET shall be rated for 1000BaseT speeds.

FO's requiring faster speed may utilize higher speed networks, such as 10GbE (10 gigabits/second), as needed.

5.1.3.6 SECNET topology shall, at a minimum, consist of the following:

- Border Router(s)/Switch(s)
- LAN/WAN firewall appliance
- IDS/IPS security appliance(s)
- Internal access layer switches

5.1.3.7 Where SECNET data transits a WAN, backbone or public network it shall be protected with encryption either using a VPN tunnel or AES256, or better, encrypted data.

5.1.3.8 Wi-Fi connectivity may be used by mobile devices to connect to SECNET when required for emergency response management as long as it complies with the following:

- All mobile devices authorized for access to SECNET must be enrolled in a Mobile Device Management (MDM) system.
- Secure Sockets Layer/Transport Layer Security (SSL/TLS) shall be used to encrypt all data transmitted across the Wi-Fi network.
- Wireless Access Points (WAP) shall be implemented using internal enterprise WAP devices.
- Mobile devices shall not use the Wi-Fi network to connect to the internet. Connectivity shall be limited to the facility network.

5.2 Wireless Communications

Wireless technologies shall be used by security personnel for voice, data and video communications that are required for emergency response management at a facility.

5.2.1 **Government Approvals**

FO is responsible for securing approvals from Communications Information Technology Commission (CITC), and other relevant Saudi Government agencies, for frequency allocations, import permissions, installation and use of wireless radios and related devices.

5.2.2 **Voice**

Wireless systems used for voice communications may consist of base stations, vehicle mounted radios and handheld radios.

5.2.2.1 All radios shall be intrinsically safe for use in hazardous environments as specified in SAF-12.

5.2.2.2 All radio equipment shall be addressable and capable of being formed into structural groups. FO shall have the capability of disabling a radio from accessing a group.

The FO shall have the capability to add, or delete, a radio from any group at any time to prevent that radio from receiving further voice communications from the group.

All voice radio communications equipment shall have at least four channels/groups for security, firefighting, emergency response and operations.

5.2.2.3 All radio communications shall be encrypted using encryption keys or similar schema. The decryption keys shall be retained by the FO.

5.2.2.4 The radio system shall have the capability to access other systems in case of emergencies when required by the FO. FO shall determine the requirements.

5.2.2.5 Selection of the type of emergency by the operator shall cause generation of a series of distinctive audio tones which alert users to the existence of an emergency.

5.2.2.6 Radio equipment selected by the FO shall comply with the following:

- The vehicle radio equipment shall be capable of interfacing with a vehicle and sounding the horn upon receiving an incoming call or using a loud speaker installed on the vehicle as a public address system.
- All radio equipment shall be approved for operation in environmental conditions specified in SEC-01.

نسخة مرخصة لشركة الهيئة الوطنية

- The selected radio system shall be capable of interfacing to external command and control systems, such as at an SCC, where the integration of security systems are required.
- The radio equipment shall have the capability of being used with protective clothing & gloves worn by disaster control teams in cases of emergency.
- Comply with the requirements of IEC 60529 & 62305 for sealing & lightning protection.

5.2.2.7 The FO shall ensure that adequate supply of portable radio systems is provided to meet routine demands and cases of emergency. Additional numbers of radio equipment shall also be made available in cases of emergency for use by external agencies that may require them to respond to an emergency.

5.2.2.8 The radio system design shall incorporate adequate capability to deal with major increases in communications requirements during an emergency.

5.2.2.9 FO shall ensure that the installation of the radio systems complies with the following:

- Communication towers required by the radio system shall fully comply with the requirements of TIA-222-G.

  Towers that are not within the facility secured perimeter shall be enclosed by an internal separation fence as defined in SEC-02.
- FO shall ensure that all radio equipment has clear coverage in its operating areas and security facilities. This includes coverage inside structurally insulated buildings and in control rooms.
- All radio system related installation shall comply with applicable TIA and IEC standards.
- Structures housing communications and network equipment for compliance with this directive shall meet the requirements of SEC-09.
- All wireless voice communications shall be recorded and kept for 12 months as specified in SEC-05.

- Local availability of services and spare parts by the supplier or agent for the useful life of the system shall be guaranteed by the contractor implementing the project.

5.2.2.10 FO shall follow the following 3-step workflow for HCIS approvals of radio equipment;

A. FO submits wireless equipment data for approval to HCIS as follows:
   - Datasheets for handheld, vehicle and desktop wireless equipment showing the specific communications equipment make, model, parts list, and manufacturer's catalog.
   - Equipment operational temperature rating compliance with SEC-01 environmental rating.
   - Quantities of each equipment type.
   - Deployment plan.

B. HCIS must review and concur with any requests for CITC approval of frequency allocations for wireless radio equipment that is covered under this directive.

C. Facility operator submits documentation to HCIS as follows as part of Stage 4 submission, or earlier:
   - CITC approval copy.
   - Radio coverage map showing adequate coverage in all areas including buildings.

FO shall note that HCIS only reviews the radio system technical compliance with SEC-08 requirements. All other permissions are acquired from CITC and other government agencies.

5.2.3 **Data**

Any wireless device covered by this directive that transmits or receives data shall comply with the requirements stated in section 5.2.2 of this directive.

5.2.4 **Video**

Any wireless device covered by this directive that transmits or receives video shall comply with the requirements stated in section 5.2.2 of this directive.

5.2.5 **Automatic Vehicle Location**

Any wireless device covered by this directive that transmits or receives AVL data shall comply with the requirements stated in section 5.2.2 of this directive.

FO may use satellite based AVL systems where required. AVL data shall comply with the requirements stated in section 5.2.2 of this directive while in transit across any public network.

5.3 Power Supply

5.3.1. Power supplies for wired and wireless security communications and network infrastructure equipment shall comply with the requirements of SEC-07, IEC 60086 and IEC 60255.

5.3.2. Security communications equipment shall be powered by the same dedicated UPS that supplies all security equipment as specified in SEC-07.

5.3.3. Where the UPS specified in 5.3.2 is not available, FO shall install a dedicated UPS for security related communications equipment. This UPS shall comply with SEC-07 requirements.

5.4 Maintenance & Support

FO shall implement a documented procedure for support and maintenance of security communication systems and components in compliance with SEC-15.

5.5 Security

All communications and network equipment covered by this directive shall comply with applicable requirements of SEC-12; Cybersecurity.

نسخة مرخصة لشركة المياه الوطنية

6 Application of Requirements

This section lists how the elements of this security directive apply to facilities depending on their Facility Security Classification (FSC) as defined in SEC-01.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Wired Communications	✓	✓	✓	✓	
Wireless Communications	✓	✓	✓	✓	
Power Supply	✓	✓	✓	✓	
Maintenance & Support	✓	✓	✓	✓	
Security	✓	✓	✓	✓	

نسخة مرخصة لشركة المياه الوطنية

7 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

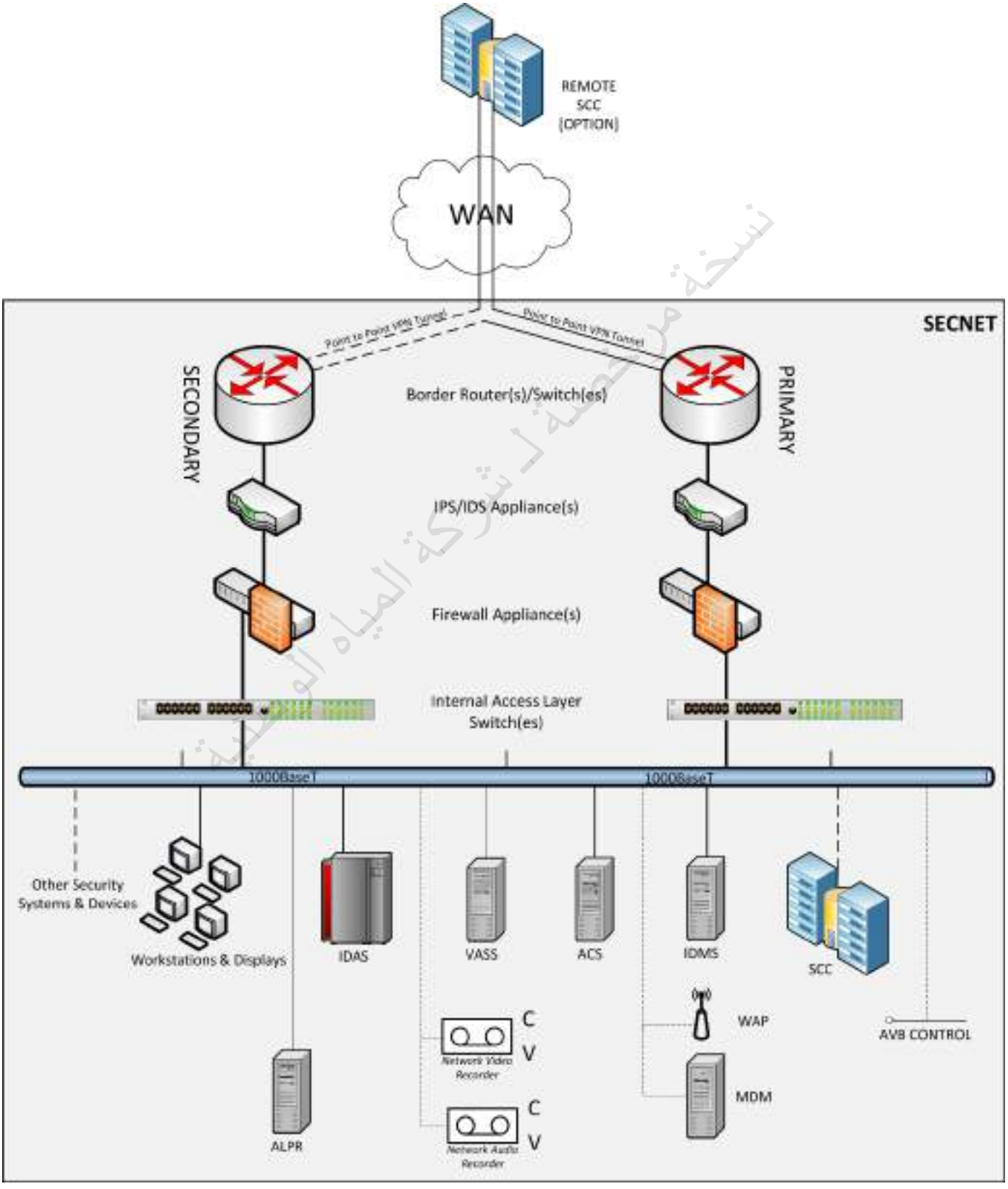
This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-08 Reference	Requirement	FO Response
1.	5.1.2	Voice	*List number of hotlines and telephone lines*
2.	5.1.3	Data	*Provide details to show how submission complies with 5.1.3 requirements* *Provide main device datasheets*
3.	5.2.2	Wireless Voice	*Provide details to show how submission complies with 5.2.2 requirements*
4.	5.3	Power supplies	*Provide details to show how submission complies with 5.3 requirements*
5.	5.4	Maintenance & Support	*Provide details to show how submission complies with 5.4 requirements*

نسخة من خطة المملكة للمياه الوطنية

APPENDIX A: SECNET OVERVIEW DIAGRAM



نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-09

Structures Housing Security Equipment

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Effective Date
1	Original Issue	• 12 Jumada II, 1431 • 26 May, 2010
2	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

**This directive was originally entitled Security Doors. The content from the original directive, as well as SEC 10 (Security Locks) has now been incorporated into this directive which now has a revised name.*

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

Table of Contents

1. PURPOSE 6

2. SCOPE 6

3. ACRONYMS & DEFINITIONS 6

4. REFERENCES 6

5. GENERAL REQUIREMENTS 8

5.1. STRUCTURES 8
5.2. SECURITY CONTROL CENTER (SCC) 9
5.3. DOORS 10
5.4. LOCKS 13
5.5. KEYING SYSTEMS 15

6. APPLICATION OF REQUIREMENTS 15

7. PROOF OF COMPLIANCE (POC) 16

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1. Purpose

This document provides requirements for structures housing security equipment.

2. Scope

This directive provides Facility Operators (FO) with the requirements for designing and implementing structures for deployment of security systems at industrial facilities under the jurisdiction of the HCIS.

3. Acronyms & Definitions

ACS	Access Control System
CMU	Concrete Masonry Unit
FDC	Field Distribution Cabinet
FO	Facility Operator: the owner, operator or lessee of a facility
HCIS	High Commission for Industrial Security
PCR	Plant Control Room
PIB	Plant Interface Building
SCC	Security Control Centre
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation

4. References

This directive adopts the latest edition of the references listed.

ASTM A879 / A879M	*Standard Specification for Steel Sheet, Zinc Coated by the Electrolytic Process for Applications Requiring Designation of the Coating Mass on Each Surface*
ASTM B16	*Standard Specification for Free-Cutting Brass Rod, Bar and Shapes for Use in Screw Machines*
ASTM B30	*Standard Specification for Copper Alloys in Ingot Form*
ASTM B505	*Standard Specification for Copper Alloy Continuous Castings*
ASTM B584	*Standard Specification for Copper Alloy Sand Castings for General Applications*
ASTM B770	*Standard Specification for Copper-Beryllium Alloy Sand Castings for General Applications*
ASTM E18	*Standard methods for rockwell hardness and rockwell superficial hardness of metallic materials*
ASTM F1135	*Standard Specification for Cadmium or Zinc Chromate Organic Corrosion Protective Coating for Fasteners*
ASTM F883	*Standard Performance Specification for Padlocks*

نسخة من خصائص المياه الوطنية

ASTM F3038 -14	*Standard Test Method for Timed Evaluation of Forced-Entry-Resistant Systems*
BS EN 1303:2005:1998	*Building Hardware – Cylinders for locks – Requirements and Test Methods*
ISO 11064: 1-7	*Ergonomic design of Control Centers*
NIJ 0108.01	*National Institutes of Justice Standard 0108.01* *Ballistic Resistant Protective Materials*
SAF-04	*Fire Protection Systems & Equipment*
SAF-20	*Pre-Incident Planning & Management of Emergencies*
SEC-01	*General Requirements for Industrial Security*
SEC-05	*Security Systems at Industrial Facilities.*
SEC-07	*Power Supply*

نسخة مرخصة لشركة المياه الوطنية

5. General Requirements

Security systems deployed at industrial facilities, under the jurisdiction of the HCIS, shall be housed in structures that comply with the requirements stated in this directive.

5.1. Structures

Security systems shall be housed in secured structures that have adequate structural, electrical and environmental safeguards.

Security system components may be housed in dedicated rooms within an existing structure or in dedicated structures. In all cases, the structures shall meet the requirements listed in this directive.

5.1.1. **Structural Constraints**

Structural constraints include ballistic protection.

- Structure shall comply with the requirements of SAF-20.
- The walls shall have ballistic protection to NIJ 0108.01 Level III. FO may use any of the methods described below:
  - Reinforced concrete walls with a minimum thickness of 205 mm.
  - Concrete Masonry Unit (CMU) construction with rebar and grout in each core.
  - Prefabricated panels with a minimum thickness of 205mm with rebar reinforcement.
- No windows shall be permitted in the area of the structure housing security system or SCC components.

5.1.2. **Field Distribution Cabinet (FDC)**

- All security related equipment, terminations and cabling installed in the FDC shall be rated to operate in the environmental requirements specified in SEC-01 as well as predicted internal temperature conditions when the FDC is exposed to direct sunlight.
- Doors to the FDC shall have tamper sensors that are connected to the SCC and shall annunciate an alarm when the FDC is accessed.
- All FDC openings shall have adequate weather sealing to prevent the ingress of water, moisture or dust into the FDC.
- All FDC's shall be locked with locks complying with the requirements stated in section 5.4 of this directive.

- FDC's shall be located within the secured facility perimeter.

5.1.3. **Access**

Ingress into a structure housing security system components shall be via a steel door fully compliant with the requirements stated in section 5.3 and 5.4 of this directive. Access to these locations shall be restricted to authorized personnel only.

5.1.4. **Environmental**

Structures shall have two separate, independent air conditioning systems as specified in SEC-01.

5.1.5. **Power Supply**

The power supplies for security systems in applicable structures shall be fully compliant with the requirements stated in SEC-07.

5.1.6. **Clearances**

The room shall be sized such that, with all equipment installed there shall be a minimum of 1.5m clearance in all directions to allow for operational and maintenance access.

Wall mounted equipment shall require this clearance in front and sides only.

5.2. Security Control Center (SCC)

Structures housing the SCC shall comply with the requirements listed below;

5.2.1. SAF-04 compliant fire detection and fire protection systems shall be installed in the SCC.

5.2.2. The SCC operator work area shall have no offices other than those required for SCC personnel.

5.2.3. The SCC shall be sized to accommodate large screen displays, multiscreen work consoles, video walls and other devices required for SCC operations.

5.2.4. The SCC operations area shall have raised floors to facilitate the installation of cabling.

5.2.5. The sizing and layout shall fully comply with the requirements of ISO 11064 (Ergonomic Design of Control Centers) sections 1 through 7.

5.2.6. All security equipment shall be housed in a separate room. Access to this room shall use the ACS and require SCC operator approvals of all access requests.

5.3. Doors

Doors used in structures housing security systems shall comply with the requirements listed in this section.

5.3.1. **Door Types**

The doors covered by this directive are defined as follows:

5.3.1.1. Entrance Door

Any door leading into an area of a facility where the following facilities or services are located:

- Security systems
- Security Control Center
- Facility Plant Control Room (PCR)
- Facility Plant Interface Building (PIB)

5.3.1.2. Exterior Door

Any doors on the outside of a building where security systems are located.

5.3.2. **Door Specific Requirements**

This section details any special requirements for each door type. Requirements common to all doors can be found in section 5.3.3 of this directive.

5.3.2.1. Entrance Door

There are no special requirements for this door type. These doors need to meet the common requirements stated in section 5.3.3 of this directive.

5.3.2.2. Exterior Door

Exterior doors shall have bollards or other barrier to prevent a vehicle from ramming the door. FO shall consider using additional interior security doors to increase the protection of the facility.

5.3.3. **Door Common Requirements**

The requirements stated in this section apply to interior doors, exterior doors and emergency exit doors covered by this directive.

5.3.3.1. Structural

5.3.3.1.1. Doors & mounting hardware shall be certified to comply with the ballistic protection requirements of NIJ 0108.1 Level III. The certification shall be traceable to an internationally recognizable authority.

5.3.3.1.2. All door components shall provide the same level of protection as the door. This includes frame, hinges and fasteners.

5.3.3.1.3. Steel used in the door shall be of the type, thickness and strength to meet all applicable requirements of this specification.

5.3.3.1.4. On an outward opening single leaf door any clearance between the lock stile and the door frame to be covered by an external, mild steel plate to cover the lock bolt in the thrown position.

5.3.3.1.5. Any clearances on double leaf door shall be fitted with external and internal mild steel strips extending the full length of the meeting stiles.

Double door systems shall have locking systems that secure the door top and bottom in each leaf of the door. A removable mullion shall be used to improve the doors structural strength.

5.3.3.2. Hardware

5.3.3.2.1. Hardware like bolts, screws, nuts, and similar shall be high-quality and corrosion protected to ASTM F1135 or equivalent.

5.3.3.2.2. All steel sheet used shall be corrosion protected to ASTM A879/A879M or equivalent.

نسخة مرخصة لشركة الباه الوطنية

5.3.3.2.3. Doors shall have the capability of installing sensors that can be tied into the intrusion detection system specified in SEC-05.

5.3.3.3. Frame

5.3.3.3.1. The door frame shall be considered a part of the door for purposes of entry resistance testing and shall afford the same security and ballistic protection as that of the door.

5.3.3.3.2. The door frame shall be attached to sub frames that are embedded into the surrounding concrete walls or attached to other structural wall material.

5.3.3.3.3. The frame shall be designed so that when attached to the wall, the wall clamping bolts shall be exposed only on the inside of the room.

5.3.3.3.4. Doors, frames, and keepers shall be strictly anchored and provided with anti-spread space filler reinforcement to prevent disengagement of the lock bolt by prying or jacking of the door frame.

5.3.3.4. Hinges

5.3.3.4.1. Doors shall be mounted to the frame by not less than three hinges or a continuous hinge, designed to allow the door to be opened approximately 180 degrees.

5.3.3.4.2. Hinges shall be rated for continuous operation for the actual weight of the door.

5.3.3.4.3. Hinges and hasps are to be attached to the doors by welding, riveting or bolting (nuts on inside of door). They are to be installed in such a manner that the hinges and hasps cannot be removed when the doors are closed and locked. Their construction to be such as to prevent removal of the hinge pin from the outside.

نسخة غير خاضعة لنظام الوطنية

5.4. Locks

The requirements specified in this section apply to locks and padlocks used to secure the following:

- Security systems
- Security Control Center
- Facility process control room
- Security equipment cabinets
- Field Distribution Cabinets
- Security gates

5.4.1. Door Locks

5.4.1.1. Lock shall be a deadlock action type lock. This type of lock shall incorporate a deadbolt.

Dead bolt shall be not less than 1" (25 mm) throw with saw-resistant hardened steel insert.

5.4.1.2. Lock cylinders shall comply with the requirements of Grade 4, or higher, of BS EN 1303 lock cylinder to have 30,000 possible different key combinations, a minimum of 5 movable levers, pins, discs, etc., and resist 15Nm of "plug" torque.

5.4.1.3. Lock cylinders shall comply with the requirements of Grade 4, or higher, of BS EN 1303 Grade 1 attack resistance grade requirements.

5.4.1.4. Fixing screws shall be hidden when the door is closed.

5.4.1.5. The lock bolt shall be made of Type 304 stainless steel or equivalent material that is corrosion resistant, and has a hardness of at least Rockwell B85.

5.4.1.6. Rockwell hardness shall be defined by the methods specified in ASTM E18.

5.4.1.7. Lock shall be mortised into fabric of door.

5.4.1.8. Protection for the extended locking bolts shall be built into the door frame.

نسخة مرخصة لشركة الهيئة العالمية

5.4.2. Padlocks

5.4.2.1. Padlocks shall use deadlock action.

5.4.2.2. Case shall be uniformly case hardened steel with hardness in range of 40 to 50 on the Rockwell C scale (40-50 HRC).

5.4.2.3. Case shall protect shackle on three sides.

5.4.2.4. Shackle, case spring and attachments shall be in accordance with the following:

- If shackle is made of brass or bronze, it shall comply with the requirements of any one of the following ASTM standards; ASTM B16, B30, B505, B584, or B770.
- Corrosion resistant steel, carbon steel or alloy steel may be used as required in commercial practice unless specified otherwise.
- Steel shackle shall be uniformly case hardened and shall meet the minimum desired grade requirements as specified for Forcing Tests of ASTM F883.

5.4.2.5. Padlocks shall use a minimum five tumbler cylinder level.

5.4.2.6. All keys shall be captive (i.e. key cannot be removed) in the cylinder when unlocked.

5.4.2.7. Key shall rotate a minimum of 90° to engage or disengage the lock.

5.4.3. **Lock Common Requirements**

5.4.3.1. All locks shall be designed to operate in the environmental conditions specified in SEC-01 “Application of Security Directives”.

5.4.3.2. All Keys shall be a nickel silver key or better.

5.4.3.3. All Keys shall be stamped “DO NOT DUPLICATE”.

5.4.3.4. Key shall not break under an applied of 2.5 Nm.

5.4.3.5. Lock cylinders mounted in door frames/doors shall have similar capabilities in their resistance to forced entry.

5.4.3.6. Gates that require padlocks for compliance with this directive shall have all hasps, shackles and fastening hardware hardened to the same level as the padlocks used to secure the gate.

5.5. Keying Systems

Locks shall have a formal keying system in place to track keys and locks as specified below:

5.5.1. Grand master keys shall not be permitted. Grand master keyed means that the grand master key can open all locks within all groups making up the set.

5.5.2. Master keys used in locks deployed for compliance with this Security Directive requires that the master key shall open all locks in a group, but shall not open locks of another group.

5.5.3. Lock sets that have more than one (1) group shall be equipped with two (2) keys per lock and two master keys per group.

5.5.4. Master keys shall have individual serial numbers. Owner shall retain a written list of personnel who have been issued these keys.

5.5.5. Where padlock set that have more than one (1) group, the set shall be equipped with two (2) keys per lock.

5.5.6. Key/padlock combinations shall be selected such that no key shall operate more than 1 padlock out of 50 padlocks.

5.5.7. FO shall maintain strict accountability of key distribution and management.

6. Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Physical Structure	✓	✓	✓	✓	
Visual Elements	✓	✓	✓	✓	
Entrance Door	✓	✓	✓	✓	
Exterior Door	✓	✓	✓	✓	
Common Requirements	✓	✓	✓	✓	
Door Locks	✓	✓	✓	✓	
Padlocks Gates	✓	✓	✓	✓	
Lock Emergency Exit Door	✓	✓	✓	✓	
Common Requirements	✓	✓	✓	✓	
Keying system	✓	✓	✓	✓	

7. Proof of Compliance (PoC)

FO shall provide HCIS with a Proof of Compliance (PoC) as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-09 Reference	Requirement	FO Response
1.	5.1	Structures	*Submit overview how security facilities comply with the requirements of this section*
2.	5.2	SCC	*Submit compliance listing with details to show how the SCC complies with these requirements.*
3.	5.3	Doors	*Submit compliance listing with details to show how the relevant doors comply with these requirements.*
4.	5.4	Locks	*Submit compliance listing with details to show how the locks on relevant doors comply with these requirements.*
5.	5.5	Keying Systems	*Provide information on keying systems being deployed for access to areas designated in section 5.4, para 1.*

نسخة من هيئة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-10

Railway Operations in Industrial Facilities

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0*	• 5 Rajab, 1438 • 2 April, 2017

**SEC 10 was originally titled Security Locks. The content from that directive has now been incorporated into SEC-09 now titled Structures housing Security Systems*

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1. PURPOSE 7

2. SCOPE 7

3. ACRONYMS & DEFINITIONS 7

4. REFERENCES 8

5. GENERAL REQUIREMENTS 9

5.1. Introduction 9
5.2. Railway Security Operation Plan (RSOP) 9
5.3. Perimeter Security 9
5.4. Railway Track Construction 10
5.5. Interference with Security Systems 11
5.6. Railway Rolling Stock Security 11
5.7. Coordination Requirements 11
5.8. Emergency Planning 12
5.9. HAZMAT Management 12
5.10. Communications 13

6. APPLICATION OF REQUIREMENTS 14

7. PROOF OF COMPLIANCE (POC) 14

نسخة من رخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1. Purpose

The purpose of this document is to provide security requirements for the use of railway services within an industrial facility.

2. Scope

This standard details security requirements at facilities where the FO utilizes railway services that penetrate the facility perimeter.

This directive only covers the specific requirements applicable to railway operations at Industrial Facilities. All other requirements stated in SEC-01 through SEC-19 continue to be applicable.

3. Acronyms & Definitions

AVB	Anti-Vehicle Barrier: There are three types of AVB: • Deployable AVB: *This type of AVB is deployed at gates in the vehicle traffic lanes & is commonly referred to as a* Road Blocker. • Fixed AVB: *This type of AVB is deployed as part of the perimeter fencing system* • Bollards: *Bollards may be fixed or deployable. They are required for traffic management and roadway containment in the gate area.*
CoC	Chain of Custody
FO	Facility Operator
FRG	Facility Railway Gate
HAZMAT	Hazardous Material
HCIS	High Commission for Industrial Security
IDAS	Intrusion Detection & Assessment System
PoC	Proof of Compliance
RSOP	Railway Security Operations Plan
RAC	Railway Activities Coordinator
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
SRA	Security Risk Assessment
VASS	Video Assessment & Surveillance System
VVTT	View, Verify, Tug & Twist

4. References

This directive adopts the latest edition of the references listed.

FO shall note that these references are provided to assist FO in the development of a viable security and safety strategy as pertains to railway operations within facility perimeters.

The FO shall utilize these references to develop a viable Railway Security Operation Plan (RSOP) that will address all security and safety concerns while complying with relevant national KSA standards for railway operations.

ISO 17712	*Standards for High Security Seals*
SEC-01	*Security Directives for Industrial Security*
SEC-05	*Security Systems at Industrial Facilities*
SEC-15	*Security Management at Industrial Facilities*
SAF-02	*Environmental Health and Safety Management*
SAF-20	*Pre-incident Planning and Management of Emergencies*
SAF-24	*Hazardous Material of Portable Containers*

نسخة من الشركة المياه الوطنية

5. General Requirements

5.1. Introduction

FOs utilizing railroad services at industrial facilities under the jurisdiction of HCIS must comply with the requirements listed in this directive when the railway penetrates a facility perimeter classified in accordance with SEC 01. Once the train approaches and penetrates the perimeter, HCIS requirements stated in this directive shall apply.

The impact of the railway operation on the facility security and its perimeter shall be covered and based on the facility SRA.

5.2. Railway Security Operation Plan (RSOP)

FO shall develop a RSOP for the facility that identifies and addresses all security and operational related issues. The RSOP shall address and include each of the following:

- Perimeter Security
- Railway track alignment within industrial facilities
- Existing security systems
- Railway rolling stock security
- Coordination with railway operator & government security forces
- Emergency Planning
- HAZMAT Management
- Communications

5.3. Perimeter Security

FO shall ensure that the perimeter integrity and security is maintained at all times including when the train is transiting the perimeter fencing system.

5.3.1. FO shall construct a Facility Railway Gate (FRG) that will be used for train entry into the facility.

5.3.1.1. The FRG shall be manned when a train is approaching or transiting the gate.

5.3.1.2. Video surveillance cameras shall be installed at the FRG and shall be monitored at the facility SCC. These cameras shall view both sides and cover the under carriage, as well as the top of the train as it transits the gate. Cameras shall comply with SEC-05 requirements for the VASS.

5.3.2. Train passage through the perimeter shall be coordinated with the railway operator, facility security personnel and government security forces that may be deployed at the facility.

5.3.3. Train lengths shall be taken into consideration and be controlled when the train does protrude from the facility perimeter during loading and unloading.

5.3.4. FO shall secure the facility railway gate when the train is approaching and transiting the gate.

5.3.5. When no trains are scheduled for entering/exiting the facility, the gate shall be locked and the intrusion sensors shall be integrated with the perimeter IDS to maintain perimeter integrity.

5.3.6. Where applicable, the FO shall ensure that an AVB capability is installed.

5.4. Railway Track Construction

Railway track construction within the facility shall comply with the following requirements:

5.4.1. The passage of the train has the potential to disrupt seismic intrusion sensors on the facility Intrusion Detections & Assessment System (IDAS). FO shall consider the possible IDAS impact when specifying track alignment.

5.4.2. The railroad 'corridor' in facilities, where applicable, shall fully comply with applicable national requirements for railroads in all aspects including, but not limited to, the following:

5.4.2.1. Corridor width & clearances.

5.4.2.2. Signaling.

5.4.2.3. Railway crossings of roadways, design parameters, barriers, visual indicators, warnings.

5.4.2.4. Train marshalling requirements as needed.

5.5. Interference with Security Systems

FO shall ensure that existing security systems and procedures are not impacted or compromised by the train approach and passage. It may include changes in sensor layouts or sensitivity settings or revisions in procedures for maintaining security during train arrival and transit.

In all cases the functioning of security systems and procedures shall continue to comply with SEC requirements.

5.6. Railway Rolling Stock Security

The security of railway cars entering the facility must be maintained at all times.

5.6.1. Rolling stock shall be secured prior to its departure from its origin. The integrity of rolling stock security needs to be validated prior to entry into a secured perimeter. Where possible this needs to be automated to facilitate train movement.

5.6.2. Security locks and/or seals shall be installed on rolling stock. Empty & loaded rolling stock must be locked to maintain security.

5.6.3. A Chain of Custody (CoC) agreement/procedure shall be established to ensure clearly identified security responsibility from origin to destination.

5.6.4. The RSOP shall include the sealing of rolling stock and may include:

- Sealing procedures.
- Seal integrity and control as specified in ISO 17712 or equivalent.
- View, Verify, Tug & Twist (VVTT), or equivalent, based seal verification & inspection processes.

5.7. Coordination Requirements

The FO shall coordinate all railway operations that penetrate the facility perimeter, with the railway operator and local government security forces.

5.7.1. A Railway Activities Coordinator (RAC) shall be designated to coordinate all railway operations related activities with facility Industrial Security Department.

5.7.2. The procedures for identifying the train approach, authenticating its validity and approving its entry shall be clearly specified. This requires a coordinated effort between the FO and the railway operator.

5.7.3. FO shall develop the coordination plan with any government forces deployed aboard the train.

5.7.4. Train manifest, cargo content, etc. shall be verified prior to permitting train entry into the facility perimeter.

5.7.5. The request to unlock the FRG shall be made before the train reaches its safe braking distance from the FRG.

5.7.6. FO shall develop procedures for the identification of train personnel to facility security personnel.

5.8. Emergency Planning

FO shall develop an emergency response plan as described in SAF 20 (Pre-incident Planning and Management of Emergencies) for a train accident within the facility or when the train is in close proximity to the facility perimeter.

FO shall ensure that the responsibilities and functions of all participants are clearly identified to all parties concerned. These parties include the following:

- Railway operator
- Facility operators
- Local government security forces
- Industrial city management (where applicable)

5.9. HAZMAT Management

All concerned FOs shall develop coordinated procedures for managing hazardous materials (HAZMAT) as described in SAF-02 (Environmental Health and Safety Management) and SAF-24 (Hazardous material of Portable Containers) that enter the facility perimeter via railway.

5.9.1. The procedures shall consider the classification and toxicity of HAZMAT when transiting the facility perimeter.

5.9.2. They shall include any special rolling stock or transport requirements for specific HAZMAT.

5.9.3. Procedures for notification of HAZMAT related facility personnel shall be included.

5.9.4. FO shall identify HAZMAT Key Trains, Special Restricted Railcars, and Transport Restrictions in compliance with appropriate and applicable national and international rules and regulations.

5.9.5. FO shall implement appropriate HAZMAT railcar loading and unloading procedures in compliance with national regulations and the specific HAZMAT risk.

5.10. Communications

FO shall ensure they have adequate secured wireless communication capabilities to communicate with the train crew to coordinate entry into a restricted facility. FO & railway operator shall ensure that information dissemination and transmission is limited to essential information only.

نسخة مرخصة لشركة المياه الوطنية

6. Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Perimeter Security	✓	✓	✓		
Railway Track Alignment	✓	✓	✓		
Railway Rolling Stock Security	✓	✓	✓		
Coordination Requirements	✓	✓	✓		
Emergency Planning	✓	✓	✓		
HAZMAT Management	✓	✓	✓		
Communications	✓	✓	✓		

7. Proof of Compliance (PoC)

FO shall provide HCIS with a Proof of Compliance (PoC) as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-10 Reference	Requirement	FO Response
1.	5.2	Railway Security Operation Plan	*Provide RSOP for review by HCIS*

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-11

Personal Identification Verification Cards

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0*	• 5 Rajab, 1438 • 2 April, 2017

** This directive was originally named Identification Cards*

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1. PURPOSE 7

2. SCOPE 7

3. ACRONYMS & DEFINITIONS 7

4. REFERENCES 7

5. GENERAL REQUIREMENTS 8

5.1. OBJECTIVES 8
5.2. PHYSICAL STRUCTURE 8
5.3. VISUAL ELEMENTS 8
5.4. PHYSICAL CARD INTEGRITY 10
5.5. MACHINE READABLE ELEMENTS 12
5.6. ENCRYPTION 12
5.7. KEY MANAGEMENT 13
5.8. BIOMETRICS 13
5.9. CARD VALIDITY 14
5.10. CARD MANAGEMENT 14

6. APPLICATION OF REQUIREMENTS 16

7. PROOF OF COMPLIANCE 17

نسخة من رخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1. Purpose

This documents provides requirements for Personal Identification Verification (PIV) cards used by FOs.

2. Scope

This standard provides FO with the requirements for the design and issuing of PIV cards used for access to facilities under the jurisdiction of the HCIS.

3. Acronyms & Definitions

FO	Facility Operator: The owner, operator or lessee of a facility
FSC	Facility Security Classification
HCIS	High Commission for Industrial Security
HCIS RI	The Regulatory Instructions for Industrial Security in Petroleum, Industrial, Service Companies and Institutions that are Supervised by the High Commission for Industrial Security (HCIS) Issued by HCIS: 1430H/2009
PIN	Personal Identification Number
PIV	Personal Identification Verification Card
RA	Restricted Area
Shall	Indicates a mandatory requirement
Should	Indicates an advisory requirement

4. References

This directive adopts the latest edition of the references listed.

ANSI INCITS 358-2002/AM1-2007	*BioAPI Specification (Version 1.1) - Amendment 1: Support for Biometric Fusion*
ANSI INCITS 398-2008	*Common Bio Metric Exchange Formats Framework*
AES	*Advanced Encryption Standard*
ISO/IEC 14443	*Identification cards - Contactless integrated circuit(s) cards - Proximity cards*
ISO/IEC 15693	*Identification cards Contactless integrated circuit(s) cards Vicinity cards*
ISO/IEC 7810	*Identification Cards - Physical Characteristics*
NSA Suite B	*National Security Agency Suite B Cryptography*
SEC-01	*General Requirements for Security Directives*
SEC-05	*Security Systems at Industrial Facilities*

5. General Requirements

All PIV cards used for access to Restricted Area (RA) facilities and services, under the jurisdiction of the HCIS, shall comply with the requirements stated in this document.

5.1. Objectives

5.1.1. PIV cards shall be issued to individuals after proper verification of a person's identity and authorization by the FO as specified in "The Regulatory Instructions for Industrial Security in Petroleum, Industrial, and Service Companies and Institutions that are supervised by the High Commission for Industrial Security" (HCIS RI).

5.1.2. The PIV card shall only remain valid until its expiration date. A process to revoke the validity of cards shall be implemented.

5.1.3. PIV cards shall be resistant to tampering and/or counterfeiting.

5.2. Physical Structure

5.2.1. The card feedstock shall comply with the requirements of ISO/IEC 7810. This standard requires a credit card sized identification card sized approximately 85mm x 54mm. All card feedstock should be certified to comply with this standard.

5.2.2. PIV cards shall have all data directly printed on the card.

5.2.3. The card shall be protected against wear and tear by a film fused to the card surface.

5.2.4. The film shall provide visual cues that will authenticate the integrity of the printed card.

5.2.5. Data may be printed on both sides of the card.

5.2.6. While there are no restrictions on card feedstock color, it is required that the base feedstock is blank and all card details shall be printed directly on the card.

5.2.7. Data printed on the ID card shall be in Arabic & English.

5.3. Visual Elements

5.3.1. PIV card visual elements shall include, at a minimum, required data fields, company logo, usage policy statement, photograph and signature. The visual attributes should be adequate to authenticate the card in lower security applications.

5.3.2. The data fields that shall be printed on all cards, are as follows:

REQUIRED

5.3.2.1	Card Type	*Employee, Contractor, Dependent, etc.*
5.3.2.2	Last Name	
5.3.2.3	Middle Name	
5.3.2.4	First Name	
5.3.2.5	Employee Identification Number	
5.3.2.6	Government ID #	*Saudi Government ID number*
5.3.2.7	Company Name	*Contractor employees only*
5.3.2.8	Serial Number	
5.3.2.9	Expiry Date	
5.3.2.10	Blood Type	

OPTIONAL

5.3.2.11	Issue Date	
5.3.2.12	Issue Place	
5.3.2.13	Date of Birth	
5.3.2.14	Nationality	
5.3.2.15	Company C.R.	Contractor employees only
5.3.2.16	Access Rights	Restricted facility access only

5.3.3. All cards shall have the company logo imprinted on the front of the card. If required, additional logos for special cases may also be imprinted on the card.

5.3.4. Employee and contractor cards shall use clearly distinguishable color in accordance with the regulations issued by HCIS RI.

5.3.5. PIV cards in which the card holder has access to RA facilities shall use red color in a title box that identifies the card type. Red color shall not be used in title boxes or backgrounds for any other card type.

5.3.6. FO may use colored bars or indicators to designate general access rights for card holders with RA access. These general access right visual indictors shall be validated by a printed list on the back of the RA card that shows all restricted facilities where access is permitted.

5.3.7. Where the number of restricted facilities is too large to list on the back of the ID card, the FO shall use group codes to represent groups of restricted facilities where access is permitted.

نسخة مرخصة لشركة الهيئة العليا للأمن الصناعي

5.3.8. All cards must display the following printed statement on the back of the card:

This card is the property of <<insert company name>>. Use of this card, by the cardholder, or others, for purposes other than authorized by <<insert company name>> is illegal and may subject the person to criminal prosecution under the law. If found, please contact <<insert Saudi Arabia telephone number>> to arrange its return to the company.

5.3.9. The minimum size required for PIV card photographs is 40mm x 25mm in size and must allow card holder features to be clearly distinguished. The FO must ensure that the pictures are properly exposed and have adequate resolution.

5.3.10. The photographs must show a full face view with a plain, light colored background and must be located on the front of the PIV card. Personnel must not be wearing sun glasses for any PIV card photographs.

5.3.11. Where cardholder has access to RA facilities the photograph must be taken without any head gear on. Security or government personnel may use photographs with their official head gear on to clearly distinguish them from non-security or non-government personnel.

5.3.12. Photographs must be directly printed on the PIV card and also be retained within the PIV card system database.

5.3.13. Applicants shall not wear military uniform for the PIV card photograph if they are not military personnel.

5.3.14. The signature must be printed directly on the PIV card and also be retained within the PIV card system database. The signature shall be the official one used by the card holder within the company.

5.4. Physical Card Integrity

All PIV cards shall incorporate tamper resistance elements and anti-counterfeiting elements to protect physical card integrity.

5.4.1. The card shall use some form of tamper resistance that provides visual evidence of tampering. The finished card shall have all layers fused together so that removal of any layer shall not be possible without damaging other layers.

5.4.2. The card shall incorporate anti-counterfeiting measures as follows:

5.4.2.1. MANDATORY – ALL CARDS
Optical variable film (holographic film) on the front of the card imprinted with a hologram, or 3D imaging, that interacts with the base card to produce the anti-counterfeiting attribute.

5.4.2.2. PIV cards shall incorporate at least two of the anti-counterfeiting features shown below:

a. Anti-photocopy attributes
Displays images or text when the PIV card is scanned, copied or faxed.
b. Invisible UV printing
Ink visible only when exposed to UV light.
c. Micro text
Micro text involves printing very small text, usually too small to read with the naked eye, onto the note or item. Text of such small size is very difficult to reproduce accurately during attempts to counterfeit the item on which it is printed.
d. Ghost Image
A smaller version of the original photo image on a PIV Card and is generally printed semi-translucent.
e. Relief Design
A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.
f. Gullioche
A pattern of fine continuous lines which form a unique image that can only be recreated with the equipment, software and parameters used in creating the original design.
g. Optical variable ink
Color-shifting inks reflect various wavelengths in white light differently, depending on the angle of incidence to the surface. An unaided eye will observe this effect as a change of color while the viewing angle is changed. A color copier or scanner can copy a document only at one fixed angle relative to the document's surface.
h. Rainbow effects
A technique whereby two or more colors of ink are printed simultaneously to create a controlled merging of the colors, similar to the effect seen in a rainbow.

FO wishing to use alternate anti-counterfeiting techniques shall request approval from HCIS prior to finalizing the PIV card design.

نسخة مرخصة لشركة الباد الوطنية

5.5. Machine Readable Elements

The card shall include machine readable elements as a mandatory requirement.

5.5.1. All access control operations shall utilize a PIV card chip as the source for reading PIV card content. Magnetic stripes are prohibited on PIV cards used for RA access.

5.5.2. Mandatory machine readable elements shall comply with either ISO/IEC 14443A or ISO/IEC 15693.

5.5.3. Data available as machine readable shall include administrative data, access rights and biometric measurements (if used). This data shall be stored in encrypted format in the PIV card.

5.5.4. If FO decides to store access related data or logs on the PIV card, they shall also be protected by encryption.

5.5.5. PIV cards that are also used for non-RA access shall have data stored in separate containers on the PIV card chip.

5.5.6. Data encrypted on PIV card shall comply with the requirements stated in section 5.6.

5.6. Encryption

5.6.1. Data stored in PIV cards for compliance with HCIS requirements shall be protected by encryption.

5.6.2. The data encrypted on the PIV card shall be encrypted in accordance with the Advanced Encryption Standard [AES] and/or NSA Suite B.

5.6.3. Where Suite B encryption is utilized, the PIV card shall support elliptic curve key pair generation, elliptic curve private key operations and importation of digital certificates.

5.6.4. At a minimum the PIV card shall store private keys and public key certificates and perform encryption operations using the private key.

5.6.5. Encryption operations using the PIV card encryption keys shall be performed on-card.

5.6.6. The card encryption keys shall be generated on the PIV card. The PIV card shall not permit export of these keys.

5.7. Key Management

Key management deals with the secure generation, distribution, storage, and lifecycle management of cryptographic keys for PIV card credentials.

5.7.1. FO shall ensure keys are selected, distributed and stored in secure environments with the appropriate levels of encryption.

5.7.2. FO shall select a PIV card manufacturer that allows FO to utilize FO's own cryptographic authentication key ensuring a unique key for the facility or organization.

NOTE:

- *Utilizing FO's internal authentication keys protects FO from a key compromise from other readers purchased from the same manufacturer.*
- *Extracting the key from a single PIV card compromises all other PIV cards.*
- *The use of diversified keys ensures each PIV card uses a unique key that is derived cryptographically from a master key so FO's implementation is different from others.*

5.8. Biometrics

5.8.1. Biometric data used in security systems shall comply with the requirements of the latest version of ANSI INCITS 358-2002/AM1-2007 (The Bio API Specification) and ANSI INCITS 398-2008 (Common Biometric Exchange Formats Framework).

5.8.2. These standards are used to ensure interoperability of security systems by using the standard Bio API interface and standard file formats for biometric data.

5.8.3. Biometric data shall comply with all requirements stated in this directive.

5.9. Card Validity

5.9.1. The validity of PIV cards shall comply with the instructions regulating Industrial Security specified by HCIS RI. The FO may elect to have shorter validity than specified by the Ministerial Order referenced above.

5.9.2. PIV cards issued to personnel other than employees or dependents shall have expiry dates set by either of the earliest date for the following parameters:

5.9.2.1. Visa expiry

5.9.2.2. Contract expiry

In all cases PIV card validity is limited to the maximum validity specified by the Ministerial Order stated in 5.9.1.

5.10. Card Management

5.10.1. The holder of a PIV card shall be responsible for its safekeeping and shall return it prior to its expiry date or when leaving the Kingdom of Saudi Arabia.

5.10.2. The holder shall be issued with a unique personal identification number (PIN) which will allow entry to restricted areas.

5.10.3. When personnel depart on vacation, short leave or terminate their employment FO shall disable their access to restricted facilities.

5.10.4. FO shall use access control systems, as specified in SEC-05, at all restricted areas to electronically authenticate PIV cards and their access rights. RA facilities without access control shall use PIV card reader(s) to electronically authenticate the PIV card locally or centrally.

5.10.5. If authentication PIV card readers are not available at all restricted facilities then the FO shall retrieve PIV cards with restricted area access when the card holder goes on vacation or short leave. In this case, all PIV cards for RA access shall have a list of all access rights printed on the card to allow visual authentication.

5.10.6. FO shall recover penalties for lost PIV cards as specified in HCIS RI.

5.10.7. All PIV cards allowing restricted access shall be recovered from the cardholder upon termination of employment.

5.10.8. FO shall design and issue new PIV cards at least once within every 4 year cycle:

5.10.8.1. These new PIV cards design and structure shall comply with the requirements stated in this security directive.

5.10.8.2. The new PIV card designs shall be clearly distinguishable from the old PIV card designs.

5.10.8.3. New PIV card designs shall be approved by HCIS.

نسخة من خصائص كاميرا الهوية

5.10.9. Retrieved PIV cards shall be destroyed as specified in instructions regulating Industrial Security contained in HCIS RI.

5.10.10. FO shall put procedures in-place to ensure that all PIV cards provided to contractors are retrieved prior to certifying completion of a contract.

5.10.11. The FO shall implement procedures to notify all posts, where electronic access authentication is not available, regarding lost or stolen PIV cards. Notification of lost or stolen PIV cards shall be received at all posts within 24 hours of the FO being notified of its loss.

نسخة مرخصة لشركة المياه الوطنية

6. Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Physical Structure	✓	✓	✓	✓	✓
Visual Elements	✓	✓	✓	✓	✓
Physical Card Integrity	✓	✓	✓	✓	✓
Machine Readable Elements	✓	✓	✓	✓	
Encryption	✓	✓	✓	✓	
Key Management	✓	✓	✓	✓	
Biometrics	**OPTIONAL**				
Card Validity	✓	✓	✓	✓	✓
Card Management	✓	✓	✓	✓	✓

نسخة مرخصة لشركة المياه الوطنية

7. Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-11 Reference	Requirement	FO Response
1.	5.3	Card Design (Visual Elements)	*FO shall provide color images of front and back of PIV card designs*
2.	5.4.2.	Anti-Counterfeiting measures	*FO shall provide technical details on anti-counterfeiting measures that will be utilized on PIV card*
3.	5.5.5	PIV card usage for non-RA access	*If PIV card will be used for non-RA access specify how the RA & non-RA access process will be encrypted and maintained in secured containers on the card*
4.	5.6.	Encryption	*Provide responses to each item in section 5.6*
5.	5.7.	Key Management	*Provide responses to each item in section 5.7*
6.	5.8.	Biometrics	*If biometrics are used, show how section 5.8 requirements are complied with*
7.	5.10.	Card Management	*Provide responses to each item in section 5.10*

نسخة من نسخة المملكة الوطنية

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-12
Cybersecurity

Version 2.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Original Issue	• 12 Jumada II, 1431 A.H • 26 May, 2010
2	Version 2.0*	• 5 Rajab, 1438 • 2 April, 2017

** This directive was previously titled Information Protection*

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7
2 SCOPE 7
3 ACRONYMS & DEFINITIONS 7
4 REFERENCES 7
5 GENERAL REQUIREMENTS 8
5.1. Cybersecurity Managem ent 8
5.2. Risk Assessment & Management 8
5.3. Cyber Security Training & Awareness 9
5.4. Network Security Boundaries, External Connections & Remote Access 9
5.5. Access & System Security Management 10
5.6. Cybersecurity Incident Response 12
5.7. Backup & Recovery 13
5.8. Configuration Change Management 13
5.9. Data Protection Program 13
5.10. Media Disposal & Sanitization 13
5.11. Physical Protection of IA&CS Assets 13
6 APPLICATION OF REQUIREMENTS 14
7 PROOF OF COMPLIANCE 14

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document specifies the minimum cybersecurity requirements for security systems and Industrial Automation & Control Systems (IA&CS), including their communication and networking infrastructure, deployed at industrial facilities and interconnected remote facilities.

2 Scope

This directive provides the minimum requirements for companies and establishments to maintain the cyber security of deployed security systems and IA&CS.

3 Acronyms & Definitions

CSM	Cybersecurity Management
FO	Facility Operator: the owner, operator or lessee of a facility
HCIS	High Commission for Industrial Security
IA&CS	Industrial Automation & Control System
ISA	International Society of Automation
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation

4 References

This directive utilizes the latest edition of the references listed below.

ISA/IEC-62443	*Industrial Automation & Control Systems (IACS) Security Standards*
ISO 27001	*Information Security Management*
NIST SP 800-30	*Risk Management Guide for IT Systems*
NIST SP 800-34	*Contingency Planning Guide for Federal Information System*
SEC-01	*General Requirements for Security Directives*
SEC-08	*Security Communications & Data Networks*
SEC-14	*Security Project Management at Industrial Facilities*

5 General Requirements

The following requirements contain the mandatory procedural and technical methods the FO shall implement in order to protect the cybersecurity of security systems and IA&CS Assets.

5.1. Cybersecurity Management

FO shall set clear and measurable policy and procedures to protect security systems and IA&CS Assets through the implementation of Cybersecurity Management (CSM). The CSM shall be designed to protect security systems & IA&CS assets from all threats, whether internal or external, deliberate or accidental.

The CSM shall be reviewed, and updated where needed, every 12 calendar months or immediately following recovery from a cybersecurity incident. Changes to the CSM shall be reviewed by facility executive management who shall certify its compliance with facility cybersecurity requirements.

The CSM shall formally assign accountability and responsibility for cybersecurity to a designated organization.

CSM shall cover all items in this document. Changes to the CSM shall be summarized and sent to HCIS.

5.2. Risk Assessment & Management

5.2.1. The FO shall conduct and document a cyber-risk assessment that includes identification of critical IA&CS assets.

5.2.2. The FO shall address all identified risks with the appropriate treatment. Penetration testing shall be utilized as part of the risk identification process.

5.2.3. The cyber-risk assessment shall be conducted utilizing a prevailing industry methodology such as, but not limited to, the following:

5.2.3.1. NIST 800-30
5.2.3.2. ISO 27000 series
5.2.3.3. ISA 62443

FO shall identify the methodology used for the assessment.

5.2.4. A cyber-risk assessment shall be conducted either when a major change occurs to facility IA&CS or security systems or every 12 months.

5.2.5. The results of the cyber-risk assessment shall be summarized and sent to HCIS whenever the assessment is changed and shall be validated by an external audit conducted every 12 months.

5.3. Cyber Security Training & Awareness

The FO shall provide cyber security training & awareness for personnel with access to the FO's security systems & IA&CS assets. Training shall be refreshed periodically and shall not exceed 24 months between refreshers.

The FO shall ensure that personnel acknowledgment of security policies are formally documented for initial access authorization and renewed in each 24 month period or after major security policy changes.

5.4. Network Security Boundaries, External Connections & Remote Access

Network design and layout constraints for security systems are defined in SEC-08.

5.4.1. ***Network Security Boundaries***

The FO shall establish, define and document one or more Network Security Boundaries to protect IA&CS assets that are connected to a network.

The Network Security Boundary shall segregate IA&CS assets from external network connections (i.e., Business/Enterprise, third parties, the Internet, etc.) by implementing and identifying one or access control point that restricts the flow of network traffic between the Network Security Boundary and external network connections.

At a minimum, these access control points shall limit inbound and outbound network traffic to only required logical protocols, ports and services with other traffic denied by default.

5.4.2. ***Information Sharing with External Connections***

Where critical IA&CS Assets reside within a Network Security Boundary, the FO shall implement an intermediate security zone, such as, but not limited to, a DMZ to secure traffic to external systems.

نسخة مرخصة لشركة المياه الوطنية

5.4.3. ***Network Security Boundary Monitoring***

The FO shall implement security event logging and monitoring at all access control points between the Network Security Boundary and external connections.

5.4.4. ***Remote access to Network Security Boundaries***

The FO shall ensure that remote access, where implemented, to the network security boundaries shall use a documented and secured procedure that incorporates the following attributes:

5.4.4.1. Strong encryption
5.4.4.2. Event monitoring
5.4.4.3. Access controls including multi-factor authentication

5.4.5. ***Security Controls for Public Networks***

In cases where sensitive data related to the facility or IA&CS Assets traverses public networks, the FO shall ensure that such data is protected with strong encryption whilst in transit. FO shall conduct a risk analysis to determine the optimal protection strategy.

5.5. Access & System Security Management

5.5.1. ***Access Management***

The FO shall document and implement a process to authorize, based on need, physical and electronic access to IA&CS Assets and security systems. This access shall be reviewed every 12 months.

Access shall be immediately revoked when no longer needed.

Where shared accounts are required, due to IA&CS constraints or operational considerations, for access to IA&CS assets, physical technical or procedural safeguards shall be implemented by the FO.

Subject to IA&CS Asset capabilities and vendor support, the FO shall implement technical methods to enforce a limit to the number of successive unsuccessful authentication attempts.

5.5.2. Default Accounts

Subject to IA&CS Asset capabilities and vendor support, the FO shall disable unnecessary default accounts on IA&CS Assets and all security systems including default operating system level accounts.

Where default accounts are necessary, the FO shall change default passwords, subject to IA&CS Asset and security system capabilities and vendor support.

5.5.3. Passwords

Where password authentication for access to security systems and IA&CS is in use, the FO shall enforce, either through technical or procedural methods, the following password parameters:

5.5.3.1. A minimum password length that is at least twelve characters or the maximum length supported by the IA&CS asset if less than 12 characters.

5.5.3.2. A minimum password complexity that includes three or more character types: uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric, or the maximum complexity supported by the IA&CS Asset.

5.5.3.3. Passwords shall automatically expire every 6 months maximum.

5.5.4. Threat Protection and Prevention

Subject to IA&CS Asset and security system capabilities and vendor support, all IA&CS Assets and security systems shall have the latest malware protection and prevention software installed, active and maintained.

The FO shall implement methods to proactively detect and counter emerging threats.

5.5.5. Security Event Logging and Alerting

The FO shall, subject to IA&CS Asset capabilities and vendor support, enable continuous security event logging on all IA&CS Assets. This data shall be stored in a central location as well as the local site.

*5.5.6. **Security Patch Management***

The FO shall document and implement a process to manage security patches for security systems and IA&CS Assets.

Subject to IA&CS Asset capabilities and vendor support, the FO shall install the most recent security patches for IA&CS Asset and security system operating systems, firmware and software applications.

Security patches shall be installed within 4 weeks of becoming available from the vendor.

*5.5.7. **IA&CS Asset Hardening Procedures***

The FO shall document and implement security hardening procedures for all IA&CS Assets and security systems, based on industry standards and vendor guidelines, subject to IA&CS Asset and security system capabilities and vendor support.

*5.5.8. **Disable Unnecessary Services***

The FO shall disable all unnecessary features, services and associated logical network protocols and ports (e.g., scripts, applications, network services, etc.) on all IA&CS Assets and security systems, subject to IA&CS Asset capabilities and vendor support.

All security system and IA&CS workstations shall have all USB ports, CD readers and other ports to connect external devices disabled. Users shall not be permitted to install any additional software or updates.

Email services shall block any attachment that has macros or scripts.

*5.5.9. **Asset Management***

The FO shall document and review its inventory of IA&CS Assets to ensure completeness and correctness, at least once every 12 calendar months.

The FO shall ensure that any discrepancies are resolved and/or reported.

5.6. Cybersecurity Incident Response

The FO shall document and implement one or more Cybersecurity Incident response plan(s) in accordance with industry standards, such as, but not limited to, NIST SP 800-34, and FO contingency plans.

This plan shall be tested every 12 months. The results of the annual test shall be summarized and sent to HCIS.

5.7. Backup & Recovery

Back-up copies of data and software shall be taken and tested regularly in accordance with the company backup policy. Backups shall be encrypted and stored in a secured physically separate location.

FO shall have a disaster recovery plan that is periodically tested.

5.8. Configuration Change Management

All software and hardware changes to security systems and IA&CS assets shall be documented and managed through a change management process. Significant changes shall be tested to ensure they do not compromise IA&CS security controls.

5.9. Data Protection Program

The FO shall ensure that its Data Protection Program clearly assigns ownership and the responsibility, along with classification and protection of all applicable information regarding IA&CS and security systems.

5.10. Media Disposal & Sanitization

The FO shall implement and document operational procedures to ensure that electronic storage media associated with IA&CS assets or security systems are properly sanitized or destroyed prior to disposal or reuse outside of the IA&CS.

FO shall refer to related guidelines such as NIST SP 800-88 regarding media disposal and sanitization.

5.11. Physical Protection of IA&CS Assets

While this directive generally addresses the online access to IA&CS assets, the FO is also responsible for securing the physical asset as well. IA&CS assets shall be installed in secured areas or cabinets that limit access to the devices.

نسخة من نفيذ لشركة المياه الوطنية

6 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
All Requirements	✓	✓	✓		

7 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items. The Stage 3 submission, content and format are specified in SEC-14 section 6.3.

This PoC shall be submitted when available but prior to project commissioning.

This PoC shall provide details for each of the requirements listed below.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-12 Reference	Requirement	FO Response
1.	5.0	General Requirements	*FO shall provide relevant documents to validate compliance with section 5.* *Documents shall summarize each aspect of compliance with section 5.*

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-13

Facilities with Marine Interface

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Version 1.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7
2 SCOPE 7
3 ACRONYMS & DEFINITIONS 7
4 REFERENCES 8
5 GENERAL REQUIREMENTS 8
5.1 COMMON REQUIREMENTS FOR ALL FACILITIES 8
5.1.1 Device & Material Selection 8
5.1.2 Maintenance & Support 9
5.1.3 Security Risk Assessment 9
5.1.4 Establishment of a Marine Section in Industrial Security 9
5.1.5 Boat Selection 9
5.1.6 Communications 9
5.1.7 Coordination with Government Agencies 10
5.1.8 Alarm Monitoring 10
5.1.9 Access to Marine Areas 10
5.1.10 Intrusion Detection 10
5.1.11 Exclusion Zone Designation 10
5.1.12 Marine Barriers 11
5.1.13 Imaging & Detection Device Requirements 11
5.1.14 Marine Patrols 11
5.1.15 Procedures 11
5.1.16 Other Requirements 11
5.2 COASTAL INDUSTRIAL FACILITIES WITH LAND-WATER INTERFACE 11
5.3 SEAPORTS 12
5.4 OFFSHORE FACILITIES 12
6. APPLICATION OF REQUIREMENTS 13
7. PROOF OF COMPLIANCE 14

نسخة غير مخصصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This security directive provides minimum security requirements for marine facing aspects of facilities under the jurisdiction of the High Commission for Industrial Security (HCIS).

2 Scope

This Directive provides FO with specific security requirements for security implementations at facilities with a full, or partial, marine boundary. The types of facilities covered by this directive are as follows:

- Coastal industrial facilities with land-water interface
- Seaports
- Offshore facilities

3 Acronyms & Definitions

ACS	Access Control System
CG	Coast Guard
FO	Facility Operator: the owner, operator or lessee of a facility
HCIS	High Commission for Industrial Security
IMO	International Maritime Organization
ISPS	International Ship & Port Security
MIA	Marine Interface Area
PFSO	Port Facility Security Officer
PTZ	Pan, Tilt and Zoom
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
VASS	Video Assessment & Surveillance System

نسخة مرخصة لـ [illegible]

4 References

This directive adopts the latest edition of the references listed.

The selection of material and equipment, and the design, construction, maintenance, operation and repair of equipment and facilities covered by this Security Directive shall comply with the latest edition of the references listed in each Security Directive, unless otherwise noted.

SEC-01	*General Requirements for Industrial Security*
SEC-02	*Security Fencing*
SEC-07	*Power Supply*
SEC-08	*Security Communications & Data Networks*

5 General Requirements

SEC-01 through SEC-19 continue to apply to facilities covered by this directive. This directive addresses the specific requirements pertaining to marine areas of industrial facilities.

This directive is structured into 4 main sections as follows:

- Common requirements for all facilities
- Coastal industrial facilities with land-water interface
- Seaports
- Offshore facilities

5.1 Common Requirements for all Facilities

All facilities with a marine interface shall comply with the following requirements:

5.1.1 Device & Material Selection

Devices and materials selected for security related deployment in Marine Interface Areas (MIA) where they can be affected by salt spray, shall have marine area operation rated levels of corrosion protection and sealing.

MIAs are sections of the facility within 1000m of the high tide mark on the coastline.

5.1.2 Maintenance & Support

FO shall ensure that all security related imaging systems and sensors deployed in areas specified in section 5.1.1 shall have accelerated maintenance and support schedules to ensure that security devices operate at optimum levels and not have performance degraded by salt spray or other accumulations.

Additional marine specific devices, such as, but not limited to, buoys, marine barriers and boats, shall be maintained in optimum operating condition.

5.1.3 Security Risk Assessment

FO shall include a specific MIA section in the SRA that is specified in SEC-01. The MIA section shall address the protection systems, devices, detection systems and alarm annunciation systems that will be required for each element of MIA features at the facility.

5.1.4 Establishment of a Marine Section in Industrial Security

FO shall establish marine sections in local Industrial Security Departments that are responsible for managing security in the MIA. This section(s) may or may not require boats for patrols. Such determinations shall be based on the FO's internal assessment and the approved SRA recommendations for the MIA section.

5.1.5 Boat Selection

Boats selected for use by industrial security departments shall be adequately sized and powered to function effectively in the sea state generally expected in the operations area.

5.1.6 Communications

Boats deployed for compliance with this directive shall have adequate communications across the operational area and shall have the ability to coordinate operations with government marine assets.

5.1.7 Coordination with Government Agencies

FO shall develop, and implement, a coordination plan with relevant government agencies such as, but not limited to, Coast Guard, Royal Saudi Navy, Border Patrol, Facility Security Forces or other government agencies involved in securing the marine side of the facility.

5.1.8 Alarm Monitoring

All data, and alarms, from MIA sensors and imaging systems shall be monitored in the facility Security Control Center (SCC).

5.1.9 Access to Marine Areas

FO shall limit access to marine areas of the facility so that only personnel with direct work responsibilities are permitted access.

5.1.10 Intrusion Detection

Intrusion detection into the MIA shall be accomplished by a combination of long range optical cameras, thermal cameras and radar. Imagers used as sensors shall be fixed while assessment cameras shall use a PTZ mount to allow for maximum versatility.

Intrusion detection shall be automatic and result in the nearest assessment camera automatically slewing to the threat area.

Maritime VASS shall provide day & night surveillance coverage over contiguous waters surrounding the facility limits. The specifics of the threat shall be defined by the SRA as well as the minimum distance for threat detection.

5.1.11 Exclusion Zone Designation

FO shall designate exclusion zones where access is prohibited or restricted. Such exclusion zones shall be clearly marked with buoys and appropriate signage that is visible day or night. FO is responsible for ensuring that all required permissions and standard for buoy deployment are complied.

5.1.12 Marine Barriers

FO shall deploy marine barriers where needed in the MIA and at offshore facilities as long as they do not compromise facility operations or safety. The location and need for the marine barriers shall be identified in the SRA.

5.1.13 Imaging & Detection Device Requirements

Devices deployed in the MIA for compliance with this directive shall detect a threat at the following minimum ranges:

a. Radar: 3000m
b. Long Range Camera: 1000m
c. Thermal Camera: 500m

The actual range of the selected device shall be the minimum level specified above or a higher range if specified in SRA recommendations. All cameras along the MIA must use thermal cameras to complement optical cameras.

5.1.14 Marine Patrols

FO shall use industrial security boats to conduct patrols of the facility MIA, or multiple marine areas under the FO, when recommended by the SRA. This generally applies to offshore facilities and seaports.

5.1.15 Procedures

FO shall develop specific procedures for facilities covered by this directive. They shall include response plans, estimated response times, tracking personnel, boat patrol requirements, etc. that are directly applicable to MIA security.

5.1.16 Other Requirements

All relevant SEC specified requirements in SEC-01 through SEC-19 shall be fully complied with when they are directly applicable to MIA requirements.

5.2 Coastal Industrial Facilities with Land-Water Interface

FO shall take measures to ensure that the littoral areas of the MIA, seawater intakes, discharge channels and marine approaches to the facility are protected with tangible barriers.

These barriers may be fixed metal barriers at inlets or discharge pipes or floating barriers to limit access to designated section of the facility MIA. The SRA shall

consider these specific MIA vulnerabilities and recommend barrier deterrents that shall be installed.

In all cases, vulnerable areas identified in the SRA shall be monitored, and patrolled as needed, in accordance with section 5.1.

5.3 Seaports

FO shall apply aspects of the International Ship and Port Facility Security Code (ISPS), issued by the IMO, that apply to their seaports.

ISPS code application shall be based on the SRA recommendations after an analysis of facility functions within the context of ISPS definitions. FO shall note that seaports shall also be required to apply SEC-01 through SEC-19 requirements to all seaports.

5.4 Offshore Facilities

Offshore present a special case for the FO. FO shall develop procedures, designated exclusion zones & buoys (section 5.1) to protect offshore facilities.

FO shall review the facility layout and determine if any areas may be used for unauthorized boarding. These areas shall be secured within operational constraints. Surveillance cameras shall be used where needed to effectively manage security within and around the platform.

Redundancy and back-up requirements for installed security systems at offshore facilities, shall be within the offshore facility resource constraints.

FO shall examine the need for the installation of marine barriers at offshore facilities. The requirement for marine barriers shall be identified in the SRA.

6. Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Device & Material Selection	✓	✓	✓	✓	
Maintenance & Support	✓	✓	✓	✓	
Security Risk Assessment	✓	✓	✓	✓	
Marine Detachment in IS	✓	✓	✓	✓	
Boat Selection	✓	✓			
Communications	✓	✓			
Coordination with Govt. Agencies	✓	✓	✓	✓	
Alarm Monitoring	✓	✓	✓		
Access to Marine Areas	✓	✓	✓	✓	
Intrusion Detection	✓	✓	✓		
Exclusion Zone Designation	✓	✓	✓		
Imaging & Detection Systems	✓	✓	✓		
Marine Patrols	✓	✓	✓		
Procedures	✓	✓	✓	✓	

نسخة من شركة المياه الوطنية

7. Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-13 Reference	Requirement	FO Response
1.	5.1	Common Requirements	*Provide summary of compliance with common requirements*
2.	5.2	Coastal Facilities	*Provide details of canals and channels and barriers that are deployed*
3.	5.3	Seaports	*Provide summary and certifications of ISPS compliance*
4.	5.4	Offshore Facilities	*Provide list of Offshore specific procedures, drawings of exclusion zones and barrier placements and summary of surveillance camera installations*

نسخة من خطة المملكة للمياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-14

Security Project Management

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Item	Description	Issue Date
1	Version 2.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 6
2 SCOPE 6
3 ACRONYMS & DEFINITIONS 6
4 REFERENCES 7
5 GENERAL REQUIREMENTS 8
5.1. Overview 8
5.2. Planning & Execution 8
5.3. General Overview of Submission Formats 11
5.4. Submission Data Sheet 12
5.5. Electronic Formats 12
5.6. Drawing Content 14
6 SECURITY PROJECT WORKFLOW 17
6.1. STAGE 1: Security Risk Assessment & Conceptual Design 19
6.2. STAGE 2: Preliminary Design 23
6.3. STAGE 3: Detail Design 26
6.4. STAGE 4: Operational Readiness 33
7 APPLICATION OF REQUIREMENTS 37
8 PROOF OF COMPLIANCE 37

نسخة مرخصة لشركة المياه الوطنية

1 Purpose

This document provide requirements for project management of security related projects.

2 Scope

This directive provides FO with HCIS workflow and approval requirements for security related projects at facilities under the jurisdiction of the HCIS.

3 Acronyms & Definitions

ACS	Access Control System
CDD	Conceptual Design Document
COD	Concept of Design
DD	Detail Design
FO	Facility Operator: the owner, operator or lessee of a facility
FSC	Facility Security Classification
HCIS	High Commission for Industrial Security
IDAS	Intruder Detection & Assessment System
LRDAS	Long Range Detection Assessment System
ORC	Operational Readiness Certification
PD	Preliminary Design
PSI	Physical Security Infrastructure
SAT	Site Acceptance Test
SCC	Security Control Center
SDD	System Design Document
SEC	Security Directives
SECNET	Security Network
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
SOP	Standard Operating Procedure
SRA	Security Risk Analysis
VASS	Video Assessment Surveillance System

4 References

This directive adopts the latest edition of the references listed.

The selection of material and equipment, and the design, construction, maintenance, operation and repair of equipment and facilities covered by this Security Directive shall comply with the latest edition of the references listed in each Security Directive, unless otherwise noted.

ANSI/API/STD 780	*American Petroleum Institute (API) - Standard 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, First Edition, March 2013.*
CCPS	*Center for Chemical Process Safety (CCPS), Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*
ASIS RA	*ASIS International: Risk Assessment Standard ANSI/ASIS/RIMS RA.1-2015*
SEC-01	*General Requirements for Security Directives*
SEC-15	*Security Management at Industrial Facilities*

نسخة خاصة لشركة المياه الوطنية

5 General Requirements

5.1. Overview

FO shall comply with HCIS workflow submission & approval requirements for managing security related projects. These requirements cover design, development and construction or installation of any item that impacts the security posture, security systems or security infrastructure at a facility.

This directive provides the workflow, scheduling, execution, content and format of submittals that must be sent to HCIS for statutory approvals.

It is the FO's responsibility to ensure that the required data is sent to HCIS in timely fashion and in the proper sequence with the required content.

The general guidelines for FO submissions are as follows:

5.1.1 Ensure data is submitted for HCIS approvals in compliance with the workflow specified in this directive.
5.1.2 Conduct internal evaluations for HCIS compliance prior to submitting documents to HCIS.
5.1.3 Limit document content to security content unless additional data is required to clarify security requirements.
5.1.4 Ensure documents are clear & legible.
5.1.5 Do not submit extraneous documents or documents out of sequence in the HCIS workflow timeline as this shall delay the review and approval process.
5.1.6 Only include one subject in the submission.
5.1.7 Do not mix security and safety submissions under a single cover letter.

5.2. Planning & Execution

5.2.1. **Security Project Type**

Projects shall be defined in any of the three main areas shown below:

- New: New facility designed from the ground up **OR** existing facility that is being placed under HCIS jurisdiction for the first time
- Expansion: Existing facility that is being expanded
- Upgrade: Replacement of existing security components, systems or infrastructure with new items.

FO shall note that only projects that affect security systems or the security posture for the facility are subject to HCIS review and approval.

Replacement of defective or damaged security components, with the identical component, falls under routine maintenance and shall not be submitted to HCIS.

5.2.2. Project Execution Personnel

Security projects shall only be executed by qualified consultants and contractors that are approved by HCIS. Lists of HCIS approved consultants and contractors are available online at the Central Licensing Unit (CLU) website.

FO shall register at this website and utilize its resources to evaluate approved security consultants and contractors and select them for project execution.

The roles and responsibilities of security consultants and contractors that work on security related projects are listed below:

5.2.2.1. Security Consultant

Security Consultants are responsible for executing the following elements of the HCIS workflow:

- Stage 1: Security Risk Assessment (SRA) & Concept of Design (COD)
- Stage 2: Preliminary security design development & Contractor RFP preparation
- Stage 3: Review detail design & device selection developed by security contractor
- Stage 4: Monitor the following:
  - Testing & commissioning of security systems
  - Review policy, procedures and post orders implementation as developed by FO.
  - Completion of Initial training of FO security personnel on security systems operation.

نسخة غير مخصصة لتوزيع الهيئة الوطنية

5.2.2.2. Security Contractor

Security Contractors are responsible for executing the following elements of the HCIS workflow:

- Stage 3: Detail Design Development & Execution
  - Design development
  - Device selection
  - Construction
  - Installation
- Stage 4: Monitor the following:
  - Testing
  - Commissioning
  - Warranty

    (*1 year minimum after commissioning*)

5.2.3. **Security Consultant Constraints**

Security Consultants shall not partner with any company, or subsidiary, engaged in bidding on the facility security system installation and/or implementation where the consultant has executed the SRA and Preliminary Design inputs for the installation and/or implementation.

Companies selected for the role of Security Consultant are not permitted to work on, or bid for, the installation of the security system on a project in which they are the assigned security consultant.

FO's are responsible for the following:

- Ensuring that the selected security consultant has the capability, resources and assets to fulfill the role of Security Consultant and comply with HCIS related workflows and requirements.
- Consultant work output meets HCIS requirements.
- The consultant's experience and expertise matches FO project requirements.

5.2.4. Non-Disclosure Agreement

FO shall execute a Non-Disclosure Agreement (NDA) with selected consultants and contractors for each project.

نسخة من منصة أمن الصناعة الوطنية

5.3. General Overview of Submission Formats

Documents submitted to HCIS for review and approval shall be submitted as follows:

5.3.1 Only documents pertinent to HCIS review shall be submitted.

5.3.2 All drawings included in the submittal shall be referenced in the text of the design document under the relevant sections.

5.3.3 Detailed process drawings or facility layout drawings shall have non-security related elements greyed out so that the security related elements are clear.

5.3.4 Documents should be submitted in ring binders with titles on the front and spine identifying the project. The titles should include the following:

- Company name
- Project number & name
- Location
- Stage X i.e. stage 1, 2 , 3 or 4
- Volume x of x

5.3.5 Each submittal shall consist of a main document (SRA, COD, Preliminary Design, Detail Design) and supporting documents (drawings, schedules, equipment datasheets etc). The supporting documents shall be referred to in the text of the main document to provide additional details as needed.

5.3.6 Each section in the binder shall have separators clearly labeled to identify the section.

5.3.7 Drawings shall be presented in a size that is adequate to read fine details. Generally A4 sized drawings are inadequate and larger sizes shall be used. Facility layout and plot plans shall be of A0 size.

If A0/A1 or similar large sized drawings are mandatory to view facility security related items then they may be provided rolled and secured at one side.

5.3.8 HCIS evaluates submissions against the security directives and referenced international standards. All of the standards referenced in the directives are in English. In order to complete the assessment, all documents submitted for review and approval shall either be in English or have an English translation appended.

5.3.9 All documents shall have company/project information on the top of each page and page number information on the bottom of each page.

5.3.10 All documents shall be submitted as a printed hard copy and an electronic copy on removable storage media as specified in the next section.

5.4. Submission Data Sheet

All submissions at all stages should include an updated submission data sheet as shown on the next page.

This data sheet shall be the first page on all submissions.

5.5. Electronic Formats

Document soft copies presented on removable storage media shall follow the same format and sequence as in the hard copy submittal and meet the requirements shown below:

5.5.1. **Text Documents**

- Documents shall be in PDF format.
- Documents shall be complete and submitted as a single PDF file mirroring the hard copy submission.
- All soft copies of text documents shall be sized for A4 paper with the exception of drawings which shall be adequately sized for legibility.
- The documents shall be ready to print; i.e. the printable areas shall be already defined for A4 paper.
- Tables in text documents shall be structured, sized and oriented as needed to ensure printout will fit across an A4 page. Larger page sizes may be used as necessary. Multi-page tables shall have headings on top of each page.

5.5.2. **Drawings**

- All drawings shall be in high quality PDF format
- Multiple drawings on a single subject shall be included in a single, multi-page PDF file to facilitate review.
- Drawings shall have adequate size & resolution to allow review of fine details.

نسخة من نظام الأمن الصناعي

PROJECT DATA SHEET April 2016	Date:

Project Reference Number:

Company Name:	*Facility:*	FSC:
Project Title:	*Location:*	

Subject: (of this submission)

Project Scope Summary:		
ACS ☐ *(list scope summary)*	IDMS ☐ *(list scope summary)*	ALPR ☐ *(list scope summary)*
IDAS ☐ *(list scope summary)*	VASS ☐ *(list scope summary)*	LRS ☐ *(list scope summary)*
Gates & Perimeter *(list scope summary)*		
Waiver Requests *(list waiver title & reason)*		

Selected Consultant / Contractor Detail [CLU]			
Security Consultant:		*Security Contractor:*	

Submission Stage	SECURITY			Comments
	Date		HCIS Status	
	Scheduled	Sent to HCIS		
Stage 1				
Stage 2				
Stage 3				
Stage 4				
Construction*				
Comm & Ops*				

*: Facility Operator notification to HCIS, approvals not required ♦ **Comm. & Ops**: Commissioning & Operations

نسخة مرخصة لشركة المياه الوطنية

5.5.3. **Photographs**

- All photographs shall be in high quality PDF format
- Multiple photographs on a single subject shall be included in a single, multi-page PDF file to facilitate review. An example is fencing photographs.
- Photographs shall have adequate size & resolution to allow review of fine details.
- All photographs shall have captions to place them within the project context.
- Where possible, photographs shall be placed into the text documentation to permit detailed information to be provided.
- Photograph captions shall always include company name, facility name & location.

5.5.4. **Technical Brochures**

Technical brochures and manufacturer documents shall be presented in multi-page color high quality PDF files.

5.6. Drawing Content

The content of drawings submitted for HCIS compliance evaluation must include dedicated security drawings of the facility, adjacent area and security systems and infrastructure to facilitate the evaluation by HCIS.

An extensive range of information is required under each main heading shown below. The drawings can be split into multiple drawings, where needed, in order to maintain clarity of the information presented and to minimize clutter in the drawings.

As the design process evolves the degree of details in these drawings will also evolve but the general drawing subject matter will remain.

5.6.1. **Overview**

The overview drawing shall illustrate the boundaries of the facility, facilities & roads in the contiguous area and all parking facilities located externally within 100 m of any restricted area fence. The drawings shall show the boundaries and gates of the administrative and restricted areas and any planned expansions of the facility.

In areas with adjacent facilities within 1000 m the drawings shall include the boundaries and designation of these adjacent facilities.

5.6.2. **Facility Layout**

The facility layout drawings shall show the following (as applicable):

5.6.2.1. Boundary fences showing fence type, dimensions and clearances. This shall include all perimeter fences and fences around internal facilities.

5.6.2.2. Isolation Fences (for new construction) showing fence type, dimensions and clearances between the mentioned fence and the surrounding area.

5.6.2.3. External and internal security patrol roads including connections to the facility road system.

5.6.2.4. All gates showing approach roads including connections to the facility road system. Drawings shall indicate gate dimensions.

5.6.2.5. All security device locations; Security devices are drop gates, turnstiles, crash barriers, x-ray machines, cameras, and any other system deployed for security requirements.

5.6.2.6. Intrusion Detection systems installed around the perimeter. This shall include any equipment rooms or housing installed as part of these systems. All IDAS zones shall be identified.

5.6.2.7. All security system equipment, locations and physical layouts. This includes IDAS, VASS, LRDAS & ACS and all components.

5.6.2.8. Security lighting installed for security compliance (Perimeter & Check Point Lighting).

5.6.2.9. An outline of all critical assets installed within 45m of the inner fence with all dimensions. Equipment is designated as critical by the FO.

5.6.2.10. Administrative and restricted areas shall be clearly shown.

5.6.2.11. Public roads located adjacent to the facility.

5.6.2.12. Saudi Government Security Force checkpoints deployed for this facility. Clearances to the facility perimeter and road connections shall be clearly shown. If adjacent facilities are deployed for facility protection their locations shall be shown.

5.6.2.13. Gate Layout & Design. This covers all gates at the facility. Each gate shall be submitted in a separate drawing set.

5.6.2.14. Power sources and backup power services to all security facilities.

5.6.3. **Outer Perimeter Fence Crossing**

Any buried, over the fence or through the fence penetrations shall be shown in drawings.

5.6.3.1. Drawings shall show elevation views, clearances, and fence crossing details.

5.6.3.2. All culverts and drainage canals and their purpose, shall be shown in the drawings. Where pipelines utilize culverts full details shall be provided.

5.6.3.3. All cameras monitoring fence crossings shall be shown.

5.6.4. **System Drawings**

5.6.4.1. CCTV system and Field of View

5.6.4.2. Access control system layout

5.6.4.3. Perimeter intrusion detection system layout

5.6.4.4. Gate security equipment

5.6.4.5. Building security equipment

5.6.4.6. Security control center layout

5.6.4.7. Network topology & major network devices

5.6.4.8. Security communication system layout (Radio & Telephone only)

5.6.4.9. Single line diagram: power supply for security equipment (primary, alternate, UPS & emergency power generator)

5.6.5. **Device Information**

The following information shall be provided in tabular form for all security systems and devices to be installed at the facility. The table shall include the security components/device type, manufacturer, component/device model number and HCIS SEC compliance (Yes/No) for the following main system components:

5.6.5.1. Security Management System (SMS) Main Components

5.6.5.2. IDAS & VASS Main Components

5.6.5.3. Inspection Devices (X-Ray, Metal Detector etc.)

5.6.5.4. Anti-Vehicle Barriers

نسخة من خطة أمن المياه

6 Security Project Workflow

There are four security project submittals required for HCIS approval. Class 5 workflow is specified in SEC-01, Appendix C.

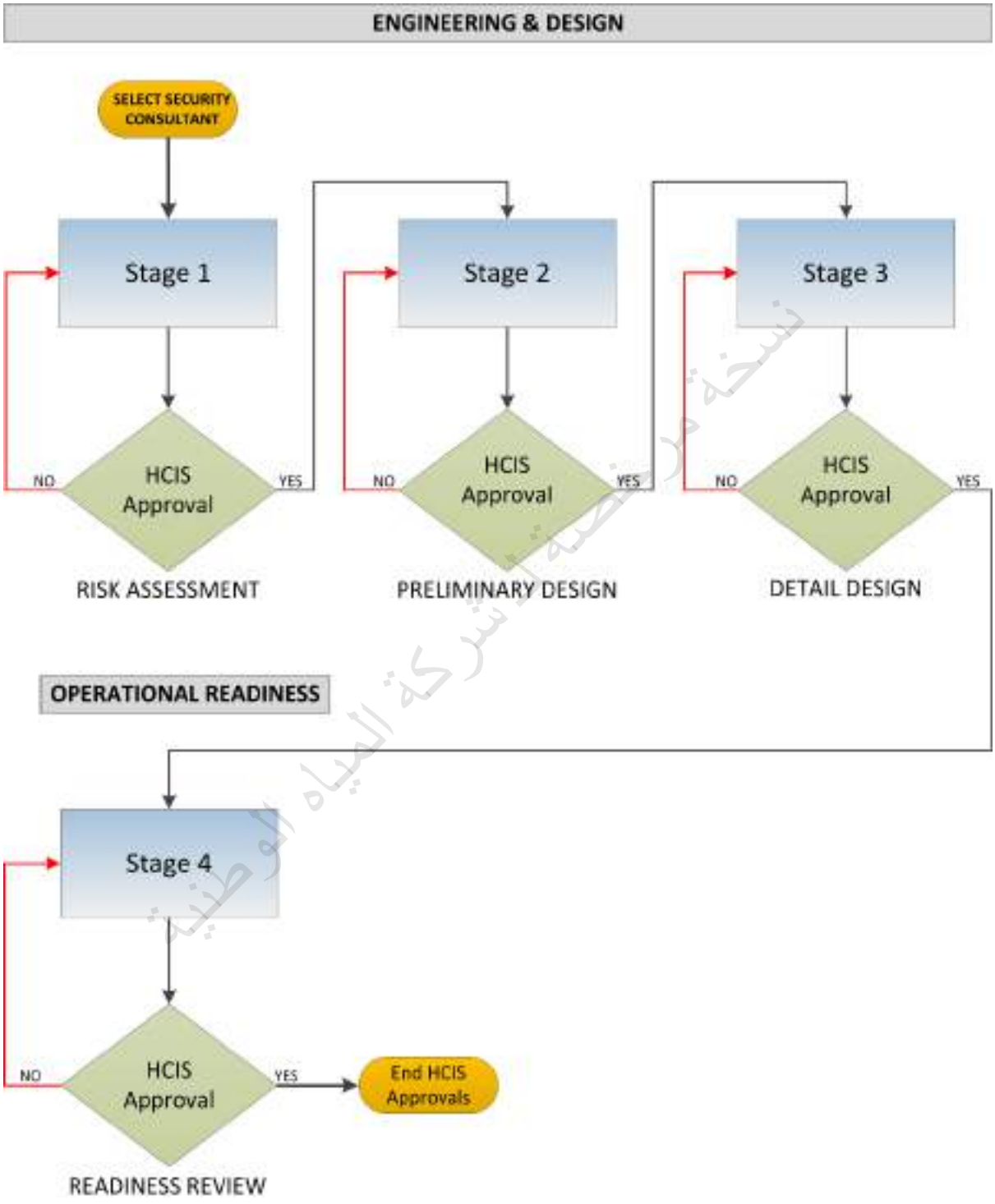
- Stage 1: Security Risk Assessment & Concept of Design
- Stage 2: Preliminary Design
- Stage 3: Detail Design
- Stage 4: Compliance & operational readiness documentation

Approval of documentation for Stage 1 through 3 is required prior to the construction, procurement or installation of any new security equipment, system or security infrastructure.

Approval of Stage 4 documentation is required during the commissioning stage of the security system but prior to declaring the facility operational.

An overview diagram of the workflow is provided on the next page.

نسخة من شركة المياه الوطنية



Security Workflow OVERVIEW

نسخة من خطة شركة المياه الوطنية

6.1. STAGE 1: Security Risk Assessment & Conceptual Design

The Stage 1 submittal consists of three parts:

- Part 1: Security Risk Assessment
- Part 2: Conceptual Design
- Part 3: Concept for Security Organization, Policy & Procedures Manual, and Training Plan development.

6.1.1. PART 1: Security Risk Assessment

The SRA is conducted and prepared by an HCIS approved security consultant. SRA requirements can be found in SEC-15, Appendix B.

A SRA shall be conducted for the entire facility which includes all new expansion areas covered by the project.

The FO shall review and approve the SRA prior to submittal to HCIS for review.

6.1.1.1. Execution & Content

Refer to SEC-15, Appendix B, section 2, 3 & 4 for requirements on SRA execution & content.

6.1.1.2. Format

The submittal content of the SRA package for HCIS review shall be Part 1 of the SRA/COD Stage 1 submittal package. It shall be clearly identified in a discrete binder as specified in section 5.3.

The SRA binder shall contain the following:

Section 1: The SRA document.
Section 2: All drawings as listed in SEC-15 Appendix B, section 3.4.2.
Section 3: Business Criteria Analysis and supporting documentation for the assessment of the Facility Security Classification.

All appendixes and documentation submitted with the SRA shall be referenced in the content and text of the SRA.

6.1.2. **PART 2: Concept of Design**

The COD translates the SRA physical security countermeasures recommendations into a more tangible conceptual overview of the physical security system and the basic layout of the security system.

The COD is the design basis for the Stage 2 Design (PD) and is prepared by the HCIS approved security consultant.

The COD is a site specific design document, defining the physical security elements and components that will be installed at the facility, where they will be installed and what are the functions of the installation. The design shall meet the FSC as approved by HCIS.

6.1.2.1. Execution & Content

The COD shall consist of a 10% Conceptual Design Document (CDD) for the physical security Infrastructure and security system with attached relevant drawings.

The CDD shall contain a complete description of the entire physical security infrastructure proposed for the project and translate all the physical security recommendations of the SRA and FSC into the design. It shall include the following:

- Summary
  An overall description of the facility and the security systems that will be installed to provide the FSC specified level of security.
- Project Overview & Site/Facility Description
- Summary from the SRA, Critical Assets, FSC & Physical Security Recommendations.
- A site specific conceptual description of the Physical Security design and security infrastructure.
- A site specific conceptual description of the security systems required for the security design of the facility.
- The COD shall include specific security countermeasures for areas where HCIS Directive compliance cannot be achieved as identified in the SRA. The FO shall include a formal request for waivers, as specified in SEC-01, for these areas in the next stage (PD).
- The specific conceptual description shall be supported and illustrated with applicable drawings as specified in section 5.6.

6.1.2.2. Format

The COD folder shall contain the following documents as indicated:

Section 1: 10% Conceptual Design Document

Section 2: Site specific drawings covering items & related equipment listed in section 5.6.

Section 3: Summary of Waiver request with justification for each non-compliance of HCIS Security Directives (If applicable) as identified in the SRA. Detailed Waiver requests shall be included in the Stage 3 submittal.

6.1.3. **PART 3: Security Org., Policy & Procedures Manual & Training Plan**

The organizational, procedural & training recommendations derived from the SRA shall be translated and developed into conceptual plans for detail development during stage 2 & 3. These documents shall be developed and prepared during stage 2 & 3 by both the selected security consultant and the FO.

The full submission shall be required in Stage 4.

6.1.3.1. Execution & Content

1. The relevant organizational recommendations shall be translated into a tangible conceptual overview for the security organization, security posts to be staffed, number of personnel required, etc.
2. The relevant procedural recommendations shall be translated into a tangible conceptual overview for the security policies, procedures & post orders.
3. A training program shall outline the formal, informal and security system training required for all security staff indicated in the security organization. The detail plan shall be developed during Stage 2 for implementation and execution during Stage 3. All training shall be completed before stage 4.

6.1.3.2. Format

The submittal content of the Security Organization, Policy & Procedures Manual, and Training Plan package for HCIS review shall form Part 3 of the SRA/COD Stage 1 submittal package, clearly identified as Part 3 and separated containing the following documents:

Section 1. Concept security organization, security posts & number of personnel required.

Section 2. Concept for development of Security Policy, Procedures and Post Orders to be developed.

Section 3. Concept for development of a formal & informal Security Training program.

For existing facilities the format shall be amended to comply with that which is described in SEC 15 Appendix A.

These documents shall be developed during Stages 2 & 3 with the final submission of the completed documents as part of the Stage 4 submittal.

نسخة مرجعية لشركة المياه الوطنية

6.2. STAGE 2: Preliminary Design

The Preliminary Design (PD) provides adequate detail of the security system design to allow the project to be bid for construction and implementation by an installation contractor.

The PD shall be executed by a qualified security consultant. The PD shall be based on the HCIS approved COD from Stage 1. The facility security design must fully comply with FSC requirements for the facility.

6.2.1. Execution & Content

The PD shall include a Preliminary Design Document (PDD) with the following minimum information:

6.2.1.1. General Requirements

The PD shall provide a summary of previous HCIS comment on the COD, a general description of the facility/site, and general project overview & requirements.

6.2.1.2. Design Criteria

1. The PD shall provide the general design criteria and specifications applicable for the preliminary design.
2. These criteria and specifications shall include, but are not limited to, compliance specifications, codes and standards for the project and the design of the security system and security infrastructure.
3. The PD shall provide the detailed requirements for the engineering design basis of the security system.

6.2.1.3. Physical Security Infrastructure (PSI) – Stage 2

The Conceptual Design Document from Stage 1 shall be developed into the Stage 2 PSI with the addition of more detail to the site specific conceptual description of the Physical Security design, security infrastructure and security management basis.

It shall provide a description for each element of the physical security infrastructure, physical security measures and technology together with the human interface and procedures required to provide the security system and organization for facility protection.

نسخة من خطة شركة المياه الوطنية

6.2.1.4. System Design Document (SDD) – Stage 2

The site specific conceptual description of the security systems required (electronic/technological components) for the security design shall be developed to a Stage 2 Security Systems design document.

It shall provide an overview of the Security Systems terminating in the SCC and integrated into the SCC environment. The section shall include a description of each system, sub-system and provide a layout of all the elements and components in the SCC. This section shall include the design requirements, specifications and operational objectives of the sub-systems and components.

All equipment and components required for the security system shall be summarized in an "*equipment identification schedule.*"

6.2.1.5. Scope of Work (SoW)

A detailed Scope of Work (SoW) shall be included to provide a clear understanding on what the security project will consist of and all the construction, installation and integration of security infrastructure and security systems required for the project that will be carried out by the Security Contractor.

This section shall describe each area and element of the security system to be constructed/installed, referencing all the specific drawings relevant to the section.

6.2.1.6. Drawings

The PD shall include a full set of drawings as specified in section 5.6 and 6.2.1.5.

6.2.1.7. Waiver Requests

The PD shall include the formal waiver requests as specified in SEC-01, section 7 and identified in the SRA & COD during stage 1.

6.2.2. Format

The submittal content of the Preliminary Design (PD) package for HCIS review shall consist of multiple ring binders clearly identified as stipulated in section 5.3.

The PD ring binder shall contain the following documents:

Section 1:
General Requirements & Design Criteria

Section 2:
PSI Stage 2

Section 3:
SDD Stage 2

Section 4:
SoW

Section 5:
Equipment Identification Schedule.

Section 6:
Waiver Requests

Section 7:
Drawings. This section shall include all drawings as applicable which consist of schematic drawings and geographic drawings.

نسخة مرخصة لشركة المياه الوطنية

6.3. STAGE 3: Detail Design

The Detail Design (DD) provides full detail of the security system design required to proceed with the construction and installation of security infrastructure & security systems by the Installation contractor.

The DD shall be prepared by the installation contractor with the oversight of the security consultant. The DD serves as the final design and specification documentation to be approved for construction and installation of the security system and infrastructure.

6.3.1. Execution & Content

The DD package for HCIS review shall only include the following:

6.3.1.1. Security Consultant review report of the detail design documentation and certificate of compliance that states the following:

6.3.1.1.1. All HCIS PD comments are incorporated into the DD

6.3.1.1.2. DD complies with the approved PD

6.3.1.1.3. DD complies with all SEC-01 through SEC 19 requirements.

6.3.1.2. A general description of the facility/site and the project overview

6.3.1.3. A detailed Scope of Work (SoW) shall be included to provide a clear understanding on what the security project will consist of and all the construction, installation and integration of security infrastructure and systems required for the project.

6.3.1.4. The Security Design Document (SDD) includes the detail design parameters, specifications and requirements for the SCC, the Physical Security Infrastructure (PSI) and all the security equipment and devices that will be installed and constructed

6.3.1.5. Detail design drawings for the security systems, security infrastructure, security buildings, security devices and equipment.

Each drawing shall be approved and certified (stamp, signature and date) by the Security Consultant as compliant with HCIS SEC Directives and the approved PD.

6.3.1.6. Vendor data sheets, specifications and certificates (where applicable) for all security devices, equipment and components.

6.3.1.7. Proof of Compliance (PoC) as specified in each directive.

نسخة غير صالحة لتقديمها للجهات الوطنية

6.3.1.8. Documentation that shows progress in the development of organizational procedures (concept Security Manual) and training programs to be conducted by the contractor and/or facility operator.

6.3.1.9. Project schedule.

6.3.2. Format

The Detail Design package for HCIS review shall consist of multiple ring binders, as stipulated in section 5.3 containing documentation as indicated below:

Each section shall contain all the documentation specific relevant to that section. Documents shall not be duplicated in other sections (such as equipment data sheets).

Section 1

General Requirements

- Security Consultant review report of the detail design documentation.
- A general description of the facility/site and the project overview.
- Detailed project description and scope of work document.

Section 2

SDD Stage 3

- Detailed SCC design documentation, the detail design parameters, specifications and requirements
- SCC Architecture description
- Function description, main requirements, architectural description and technical description for each sub-system.
- Network integration of all security sub-systems and security equipment.

نسخة مرخصة لشركة المياه الوطنية

Section 3

PSI Document Stage 3

- Detailed PSI design documentation, the detail design parameters, specifications and requirements for each building/element or equipment for the PSI
- Detailed Design drawings for the construction of all security buildings, such as gatehouses, search facilities, security control center and all buildings where security system equipment will be housed.
- Design parameters for the buildings
- Building material and equipment specifications & certifications

Section 4

Security Fencing

- Specifications, calculations & design document for installation of fencing systems considering the specific soil conditions.
- Site Perimeter Layout drawing (fence, barriers, patrol roads, lighting, clear zone, etc).
- Detailed Design drawings for the construction and installation of anti-vehicle barrier around the perimeter (Class 1 facility).
- Test report and certificate for the anti-vehicle barrier.
- Detailed Design drawings for construction & patrol road layout.
- Detailed Design drawings for the construction and installation of the facility perimeter fencing and all other fences described in the PD.
- Detailed Design drawings for each fence penetration in the facility perimeter.
- Detailed Design drawings for the layout and installation of all emergency gates and heavy equipment gates.
- Material data sheets and specifications.

نسخة من خطاب من كلية الدراسات الوطنية

Section 5

Security Gates

- Specifications, calculations & design document for layout and installation of each facility gate.
- Detailed Design drawings for the layout and installation of all security equipment, security devices, and components at each gate and in the gatehouse/search facility.
- Material data sheets and specifications.
- Test report and certificate for the crash rated road blockers & bollards.

Section 6

Security Lighting

- Specifications & design document for perimeter security lighting, each check point/gate lighting and area security lighting.
- Security lighting calculations & computer plotter prints for all perimeter, check point/gate and area security.
- Detailed Design and Installation drawings for the installation of the facility perimeter security lighting and each check point/gate lighting.
- Material data sheets and specifications.

Section 7

Security Control Center

- Detail Design drawing for the construction of the security control center with detail design parameters & specification documents.
- SCC layout
- List of systems & functions integrated into the SCC
- Integration software at SCC
- Material & equipment data sheets & specifications.
- Manning requirements

نسخة من نقطة تركيب الرياح الوطنية

Section 8

Intrusion Detection & Assessment System (IDAS)

- Detailed Design & Installation drawings for the layout and installation of the Perimeter Intrusion Detection systems.
- Detailed Design & Installation drawings for the layout and installation of the perimeter CCTV surveillance & assessment camera systems.
- CCTV camera Field of View/Lens Calculation
- Material & equipment data sheets & specifications

Section 9

Access Control System (ACS)

- Detailed Design & Installation drawings for the layout and installation of the electronic Access Control System components at each location.
- Material & equipment data sheets & specifications.

Section 10

Video Assessment & Surveillance System (VASS)

- Detailed Design & Installation drawings for the layout and installation of the Video Assessment & surveillance CCTV camera systems.
- CCTV camera Field of View/Lens Calculation.
- Material & equipment data sheets & specifications.

نسخة من منصة شركة المياه الوطنية

Section 11

Data Networks & Communications

- Data Networks
  - SECNET topology & capacity
  - Network interface equipment
  - Connection to facility backbone
  - Cabling overview & drawings for the gatehouse, SCC, ACS, IDAS and VASS locations.
  - Perimeter IDAS & VASS interface and cabling
- Communications
  - PIC wired communications
  - All Gatehouse wired & wireless communications
  - SCC wired & radio communications
  - Radio equipment list (fixed, mobile, vehicle mounted)
  - Radio coverage map
- CCTV Storage Calculations
- Communications
- Network Bandwidth Calculation

Section 12

Power Supply

- Detailed Design & Installation drawings for the Emergency Power Supply.
- Detailed Design & Installation drawings for the UPS system
- Power & UPS calculations
- Material & equipment data sheets & specifications

نسخة ترخيصة لشركة الإمام الوطنية

Section 13

- Waiver requests
- Summary of approved "Waivers" for each non-compliance of HCIS Security Directives (If applicable) as identified in the SRA & COD and previously approved by HCIS in the PD.

Section 14

Proof of Compliance

- Proof of Compliance as specified in each applicable SEC Directive.

Section 15

Operational Readiness Progress Report

- Documentation that shows progress in the development of organizational procedures.
- Training programs to be conducted by the contractor and/or facility operator for Operational Readiness.

Section 16

Project Schedule

- The project schedule shall include the start date of the project, major project milestones and project completion date.

نسخة مرخصة لشركة المياه الوطنية

6.4. STAGE 4: Operational Readiness

The final stage of the security project is the testing, commissioning and handing over of the security system for operational use to the FO.

Prior to operating the system the FO shall provide HCIS with specific documentation to illustrate that the new security system and the FO is ready to transition from the construction & installation phase to commence full operation.

6.4.1. Execution & Content

The Operation Readiness package for HCIS shall include the following:

6.4.1.1. Certifications

6.4.1.1.1. Operational Readiness Certification (ORC)

The FO & installation contractor shall jointly sign the ORC attesting the following:

- All security systems specified in the approved Detail Design are operational in all respects.
- The systems have been commissioned and tested onsite.
- Standard Operating Procedures (SOP) for the Security Department have been developed and implemented.
- Personnel have been trained to fully operate systems.
- Warranty and maintenance contracts are in place to support the systems.

6.4.1.1.2. Security Compliance Certification

FO shall submit a compliance certificate as part of Stage 4 submissions. The signatory shall be the facility CEO or facility executive management. The layout of the certificate is shown on the following page.

نسخة مرخصة لشركة المياه الوطنية

SECURITY COMPLIANCE CERTIFICATION – STAGE 4

(Submitted to HCIS by Facility Operator as part of Stage 4 submission)

Facility Operator:	*<<insert facility operator name>>*
Facility Name:	*<<insert facility name>>*
Facility Location:	*<<insert facility location>>*
Project Name:	*<<insert project name>>*

<<insert facility operator name>> certifies the following regarding the construction, installation and commissioning of all security infrastructure, systems and components implemented by the project listed above:

1. The execution of this project has been carried out as specified in the detail design approved by the High Commission for Industrial Security (HCIS).
2. The following non-compliant areas were approved by HCIS for this project:
   a. *<<insert non-compliance summary>>*
   *enter ***NONE** if there are no approved non-compliances*
3. Any unapproved deviations from the HCIS approved detail design that are designated by HCIS during a site visit or inspection shall be rectified by *<<insert facility operator name>>* in a timely manner at *<<insert facility operator name>>* cost.

Certified by: _____ _____

(Insert Facility CEO Name) (Signature)

Date: _____

Company Stamp:

Attachments:

نسخة مرخصة لشركة أبيل الوطنية

6.4.1.2. Installation & Testing

The FO shall submit the following documentation for HCIS review:

- Site Acceptance Test (SAT) results summary for all security systems implemented by the project.
- Training program, training/course contents and proof of attendance for security personnel on security system and equipment installed.
- List of SOPs for the security system installed.
- As-Built drawings (soft copy only as specified in section 5.3 & 6.3).

6.4.1.3. Facility Security Organization

The FO shall submit the following documents to demonstrate that the facility has security policies, security procedures and Security Post Orders for the security organization:

- Security Policy
- Security Procedures for the facility
- Security Post Orders for each post
- Security Staff organization chart and personnel available
- Maintenance Plan for Security Infrastructure and equipment
- Manning plan for all the security posts at the facility (i.e. gates/visitor center, SCC, Patrols etc).

6.4.1.4. Land/Water Interface:

All Facilities with a Land/Water interface shall submit a specific plan & procedure for co-operation and liaison with the Maritime Forces responsible for the protection of the marine area and assets located off-shore. The procedure shall include the communications between the role players as well as the responsibility for situational awareness, early warning and response.

SEC-13 contains additional details for such facilities.

نسخة مرخصة لدى كلية الملك الوطنية

6.4.2. Format

The Operation Readiness package for HCIS review shall consist of multiple ring binders (if required), as stipulated in section 5.3 containing documentation as indicated below:

Section 1

Certification

- Operational Readiness Certification (ORC)
- Security Compliance Certification

Section 2

Installation & Testing

- SAT Report (Summary & Certifications only)
- Training documentation
- List of SOPs for the system
- List of As-Built drawings & CD

Section 3

Security Organization

- Completed Facility Security Policy, Procedures & Post Order manual.
- Security Staff organization chart and personnel list.
- Maintenance Plan for Security Infrastructure and equipment.
- Security Posts Manning Plan.

نسخة مرخصة لشركة الدار الوطنية

7 Application of Requirements

This section lists how the requirements of this security directive apply to facilities based on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Planning & Execution	✓	✓	✓	✓	
Submission Formats	✓	✓	✓	✓	
Submission Data Sheet	✓	✓	✓	✓	
Electronic Formats	✓	✓	✓	✓	
Drawing Content	✓	✓	✓	✓	
Project Workflow	✓	✓	✓	✓	

8 Proof of Compliance

FO shall provide HCIS with Proof of Compliance (PoC) with the requirements of this Directive by submitting a completed Project Data Sheet with each submission and the specified PoC stated in each directive.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC 15

Security Management at Industrial Facilities

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Version 1.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1. PURPOSE 7

2. SCOPE 7

3. ACRONYMS & DEFINITIONS 7

4. REFERENCES 8

5. GENERAL REQUIREMENTS 9

5.1. Accountability 9
5.2. Security Risk Assessment & Management 10
5.3. Facility Security Plan (FSP) 11
5.4. Standard Operating Procedures 13
5.5. Industrial Security Department 14
5.6. Construction, Commissioning & Startup 14
5.7. Personnel Management 16
5.8. Competency & Training of Security Personnel 17
5.9. Weapons (Firearms) Control 18
5.10. Transportation 18
5.11. Maintenance & Support Program 19
5.12. Safe Work Practices 26
5.13. Management of Change 26
5.14. Incident Reporting & Investigation 27
5.15. Emergency Planning 27
5.16. Compliance Audits 27

6. APPLICATION OF REQUIREMENTS 28

7. PROOF OF COMPLIANCE 29

APPENDIX-A: TYPICAL SECURITY MANAGEMENT DOCUMENTATION 30

1.0. Introduction 32
2.0. Methodology 32
3.0. SRA Submittal Content for HCIS Review 35
4.0. SRA Format 39

نسخة مرخصة لشركة الهيدرولوجية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1. Purpose

This document provides requirements for the management of Security Operations at Industrial Facilities.

2. Scope

This directive provides the FO with requirements to manage security operations at an industrial facility using a security management system that addresses all requirements.

3. Acronyms & Definitions

COD	Concept of Design
EPC	Engineering, Procurement & Construction
ETD	Explosive Trace Detector
FO	Facility Operator: the owner, operator or lessee of a facility
FSC	Facility Security Classification
FSP	Facility Security Plan
HCIS	High Commission for Industrial Security
HCIS RI	The Regulatory Instructions for Industrial Security in Petroleum, Industrial, Service Companies and Institutions that are Supervised by the High Commission for Industrial Security (HCIS) Issued by HCIS: 1430H/2009
HVAC	Heating, Ventilation & Air Conditioning.
ISD	Industrial Security Department.
LDD	Luminaire Dirt Depreciation
LLD	Lamp Lumen Depreciation
PM	Preventive Maintenance.
PPE	Personal Protective Equipment
SCC	Security Control Center
SEC	Security Directives
Shall	Indicates a mandatory requirement
Should	Indicates a recommendation or that which is advised but not required.
SOP	Standard Operations Procedures
SRA	Security Risk Assessment
UPS	Uninterruptible Power Supply

4. References

This directive adopts the latest edition of the references listed.

ANSI/API/STD 780	*American Petroleum Institute (API) - Standard 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, First Edition, March 2013.*
CCPS	*Center for Chemical Process Safety (CCPS), Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*
ASIS RA	*ASIS International: Risk Assessment Standard ANSI/ASIS/RIMS RA.1-2015*
ASTM E2520-07	*Standard Practice for Verifying Minimum Acceptable Performance of Trace Explosive Detectors*
ASTM F792-08	*Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems*
NFPA 110	*Standards for Emergency & Stand-by Generators*
SAF-02	*Environmental, Health and Safety Management*
SAF-14	*Safe Manufacture, Transportation, Storage and use of Explosive Materials*
SAF-20	*Pre-Incident Planning & Management of Emergencies*
SEC-01	*General Requirements for Security Directives*
SEC-02	*Security Fencing*
SEC-06	*Security Devices*
SEC-08	*Security Communications & Networks*
SEC-14	*Security Project Management at Industrial Facilities*

5. General Requirements

The FO shall implement a Security Management System to address the specific security risks at each facility. It shall address each of the following issues over the entire lifecycle of the facility starting with design and construction all the way to decommissioning:

- Accountability
- Risk Assessment & Management
- Standing Operating Procedures
- Facility Security Plan
- Industrial Security Department
- Construction, Commissioning & Startup
- Personnel Management
- Competency & Training
- Weapons Control
- Transportation
- Maintenance & Support
- Safe Work Practices
- Management of Change
- Incident Reporting & Investigations
- Emergency Planning
- Compliance Audits

5.1. Accountability

A key element in implementing effective security is the concept of accountability. Personnel shall be clearly aware of their responsibilities within the security environment. Security management shall clearly designate field personnel for managing security risks in the area under their care:

5.1.1. Identify and communicate security related risks/threats to employees & contractors.

5.1.2. Communicate security rules of conduct and a Security Awareness Program to employees, visitors & contractors.

5.1.3. Provide resources for training employees for competency & security.

5.1.4. Secure compliance with security rules of conduct among employees & contractors.

5.1.5. Control contractor presence & activities in the facility.

نسخة مرخصة لشركة تمهيد الوطنية

5.1.6. Conduct regular security emergency drills & critique meetings.

5.1.7. Ensure all security incidents are reported without fear of retribution.

5.1.8. Investigate security incidents and take corrective actions to prevent recurrence.

5.1.9. Evaluate security performance by conducting regular internal/external audits as described in section 5.16 and take actions to improve performance

5.2. Security Risk Assessment & Management

5.2.1. FOs shall conduct a Security Risk Assessment (SRA) as specified in SEC-01 or as required under the conditions stated in SEC-01, section 8.3.2.

5.2.2. The FO shall review the SRA and approve the recommendations prior to submittal for HCIS review.

5.2.3. All SRA's shall be submitted for HCIS approval.

5.2.4. SRA recommendations shall provide the basis for the FSP.

5.2.5. SRA shall follow the methodology and include the information and documentation as specified in Appendix B of this directive.

5.2.6. The FO shall appoint an approved qualified security consultant to conduct the SRA as specified in SEC 01.

5.2.7. The FO shall include an action plan for the implementation of all the SRA recommendations.

5.2.8. FOs shall establish an implementation and tracking system to manage SRA recommendations, and corrective actions identified by the SRA, from implementation to completion.

5.3. Facility Security Plan (FSP)

The FO of a new or existing facility shall develop and implement a Facility Security Plan (FSP) to manage facility security during development, design, construction and operation. The FSP shall incorporate the main elements listed below:

5.3.1. FSP Overview

The FSP provides the FO with the requirements for security operations at a facility, security organization, security policy & procedures, SCC, security system & infrastructure maintenance, personnel training and a method to identify and implement required changes, enhancements or improvements to the facility security posture.

5.3.2. FSP Basis

The basis for the FSP is the SRA which is a systematic examination of the components and characteristics of facility risk as defined in SEC-01. The SRA shall provide recommendations & countermeasures for the FSP which include physical protection measures, personnel (organizational) structures and procedural measures.

The FO shall ensure that the SRA identifies and details security related changes that need to be implemented as per the SRA Recommendations. These recommendations shall be incorporated into the FSP. The FSP shall be used as the basis for infrastructure upgrades, improvements or enhancements at the facility security systems.

5.3.3. FSP Structure

The FSP structure shall incorporate the selection and integration of physical protection countermeasures, as well as procedural components recommended in the SRA to mitigate risk. It includes the following main components:

5.3.3.1. Physical protection infrastructure & security systems design.

5.3.3.2. Security program for upgrades, enhancements or improvements to existing security components or infrastructure as recommended in the SRA.

5.3.3.3. Security organization structure.

5.3.3.4. Security policy, procedures & post orders to integrate personnel & physical protection measures.

5.3.3.5. Security training program and schedule, which include security awareness training for employees.

5.3.3.6. Support & maintenance of security infrastructure & systems.

5.3.4. FSP Implementation

The FO shall implement the FSP starting with construction and continue throughout the operational life of the facility. FO shall note that the FSP applies to new projects, existing facilities and upgrades at existing facilities. In all cases, an SRA shall be carried out to evaluate and quantify the impact on the FSP.

5.3.5. FSP Support

The FO shall implement a comprehensive training, maintenance, and inspection program to ensure the proper functioning of the security infrastructure and proficiency of security personnel. The details of support requirements may be found in section 5.11.

The FSP shall be updated at the same intervals as for the SRA. These intervals are specified in SEC-01.

5.4. Standard Operating Procedures

The FO shall develop and implement written Standard Operating Procedures (SOP). They shall include, but are not limited to, the following:

5.4.1. Physical Security Procedures

5.4.1.1. Access Control
5.4.1.2. ID Card Procedures
5.4.1.3. Visitors
5.4.1.4. Contractors
5.4.1.5. Vehicle Entry Permits
5.4.1.6. Material Control
5.4.1.7. Key Control

5.4.2. Information Security & Cybersecurity

5.4.2.1. Information protection
5.4.2.2. Document Control & Security
5.4.2.3. Photography permits
5.4.2.4. Laptop & IT permits

5.4.3. Security Training

5.4.3.1. Security Training program for Security Staff
5.4.3.2. Security Awareness Training for employees
5.4.3.3. Induction of new employees
5.4.3.4. Introduction of security requirements in the safety induction on site for visitors and contractors.

5.4.4. Security Management Procedures

5.4.4.1. Security Reports
5.4.4.2. Security Statistics and Performance Measurement
5.4.4.3. Security Incident & Threat Reporting
5.4.4.4. Maintenance of Security Systems and Equipment
5.4.4.5. Emergency Response for Security Personnel
5.4.4.6. Response to Bomb Threat & Suspicious Parcels
5.4.4.7. Dealing with “Lost & Found” Items
5.4.4.8. Vehicle Accidents

نسخة من خصائص الهيئة الوطنية

5.4.4.9. Workplace violence, threats, intimidation, and other misconduct.

5.4.4.10. Contraband items

5.4.4.11. Pre-employment screening and background checks.

5.4.5. Security Post Orders

The FO shall maintain and review these procedures regularly and update them as necessary. SOP's shall always be reviewed after a major security incident or as stipulated in SEC-01 section 8.3.2.

5.5. Industrial Security Department

FO shall ensure that an Industrial Security Department (ISD) is established for facilities with a Facility Security Classification (FSC) of Class 1 through 4. A Class 5 facility may setup a smaller organization that is adequate to meet local security needs.

The Class 1 through 4 ISD shall fully comply with applicable HCIS requirements that pertain to structure, manning, manpower approvals, etc., as well as to HCIS RI.

5.6. Construction, Commissioning & Startup

The responsibility for facility security may vary through the stages of construction, commissioning and startup.

5.6.1. Construction

5.6.1.1. If project construction does not breach an operational facility perimeter and entrance to an operational facility is not required to transit construction personnel to the worksite then security shall be provided by the Engineering, Procurement & Construction (EPC) contractor for the jobsite. The construction site and access shall be isolated from the normal facility. FO may use ISD in lieu of EPC provided security at this stage if deemed necessary by HCIS or the FO.

5.6.1.2. Where construction borders an existing operational facility the construction area shall be isolated with a fence as specified in SEC-02.

5.6.1.3. Where access into a construction area requires penetration of an operational facility perimeter for the transit of personnel and material then ISD shall provide security.

5.6.1.4. During the construction of Explosive facilities, the FO shall ensure that all security related aspects applicable for these facilities shall comply with the requirements of explosive facilities construction and location as described in SAF-14.

5.6.2. Commissioning

When the commissioning process starts at a Class 1 through 4 facility, the ISD must assume all security requirements for the area being commissioned as follows:

5.6.2.1. The physical perimeter fence for the area must be complete.

5.6.2.2. Access control at all gates.

5.6.2.3. Perimeter patrols.

5.6.2.4. Liaison with commissioning team to manage special security needs.

5.6.2.5. ISD shall ensure that security personnel are trained and fully aware of any startup risks as well as the required responses.

5.6.2.6. All other security functions.

5.6.2.7. FO shall ensure that SAF-02 specified requirements for commissioning are complete.

In cases where all security systems as required by the Security Directives are not fully installed, ISD shall have adequate assets available to manually meet the above requirements.

نسخة من حصة شركة المياه الوطنية

5.6.3. Start-up

Start-up refers to the stage where a Class 1 through a Class 4 facility becomes operational and goes into production. By the time a facility reaches start-up the following security related issues must have been resolved:

5.6.3.1. All Security Directive required security systems are installed and fully operational as needed based on the FSC.

5.6.3.2. ISD personnel have all vehicles, PPE, mobile communications and other required equipment.

5.6.3.3. The Security Control Centre (SCC) is fully operational.

5.6.3.4. All gates used for access to the facility are fully manned and all equipment & services are installed and operational.

5.6.3.5. Adequate trained manpower is available to man all gates and execute all security functions.

5.6.3.6. All applicable security policies and procedures as well as post orders are available at each operational gate.

5.6.3.7. FO shall ensure that SAF-02 specified requirements for startup are complete.

5.7. Personnel Management

5.7.1. Budgeting

FO shall ensure that ISD is provided with adequate budgets and resources to meet ISD's operational needs and Security Directive requirements.

Where projects with long lead time are required for Security Directive compliance, FO shall initiate the budgeting process to ensure funds availability for project execution at the earliest possible time.

Critical recommendations in a SRA or audit report shall be addressed within the next budgetary cycle.

5.7.2. Uniforms

FO shall provide ISD personnel with uniforms compliant with HCIS requirements. Personnel shall be provided with adequate uniforms to ensure availability for applicable duty periods and shall provide cleaning services to ensure uniforms are maintained in neat and clean condition.

5.7.3. Personal Protective Equipment (PPE)

FO shall provide ISD personnel with PPE specified in SEC-06. Where personnel are expected to work inside process plants they shall be provided with PPE required for working in that specific environment.

5.7.4. Communications

FO shall provide ISD personnel with radios, compliant with SEC-08, when needed for the discharge of their duties. Spare radios and batteries shall be maintained by ISD to ensure 24hours X 365days availability of radio communications for ISD personnel.

5.7.5. Medical Fitness

FO shall specify fitness targets for security personnel. FO shall conduct bi-annual audits of security personnel fitness and ensure they meet these targets.

5.8. Competency & Training of Security Personnel

5.8.1. Personnel who are primarily responsible for site security measures (e.g., security personnel or a guard force) shall be thoroughly trained in their general and post specific duties.

5.8.2. Courses shall be developed for the target audience and delivered by competent and accredited trainers using proven training methods.

5.8.3. Skill levels shall be maintained by refresher courses at accredited national training institutions.

5.8.4. As ETD & X-ray performance frequently depends on operator skills, operators using the specific ETD or X-ray model shall be trained in its performance and use. This training shall be renewed every two years. Training shall be granted by a nationally recognized authority.

5.8.5. Training records shall be documented and tracked.

5.8.6. Training records shall be made available to HCIS upon request.

5.9. Weapons (Firearms) Control

5.9.1. FO shall ensure firearms usage by industrial security personnel comply with the following:

5.9.1.1. Personnel are evaluated for psychological stability and physical capability to handle such firearms.

5.9.1.2. Personnel are trained and qualified for handling the specific firearm.

5.9.1.3. Sufficient firearm safes are available to store firearms that are not in use.

5.9.1.4. FO shall implement a system for tracking firearms & ammunition issued to personnel.

5.9.1.5. FO shall develop policies & procedures to manage firearms at industrial facilities.

5.10. Transportation

5.10.1. FO shall provide security personnel with adequate vehicles needed to execute security tasks.

5.10.2. Security vehicles shall be clearly identified as security vehicles in compliance with relevant Saudi Government regulations.

5.10.3. Security vehicles shall be equipped with radios, sirens, spot lights and public address systems that are interfaced to the radio as specified in SEC-08.

5.10.4. FO shall ensure all personnel permitted to drive security vehicles undergo periodic defensive driving training.

نسخة من رخصة الشركة للمياه الوطنية

5.10.5. All other vehicles shall be issued with a vehicle identification pass as stipulated in HCIS RI.

5.11. Maintenance & Support Program

All security equipment shall be covered by a Maintenance & Support Program (MSP). The program shall be aimed at ensuring that security equipment and components are installed, inspected, tested, maintained, repaired and commissioned in a manner which preserves the originally intended integrity of the equipment, and by personnel who are properly trained and qualified to perform necessary activities.

5.11.1. General Requirements

5.11.1.1. The FO shall maintain the ongoing integrity of security systems and equipment.

5.11.1.2. Mitigation measures shall be put in place to maintain the security level when security equipment is out of service for any reason.

5.11.1.3. The system contractor shall provide all details and tools required for system maintenance as part of system supply. This shall include maintenance manuals, software diagnostics, special tools, calibration equipment and procedures.

The maintenance manuals shall contain recommended maintenance intervals, procedures and recommended spare parts lists.

5.11.1.4. The FO shall be responsible for implementing a maintenance strategy to meet recommended maintenance requirements for all equipment.

5.11.1.5. All components shall have regularly scheduled preventive maintenance (PM) at least once every 6 months unless required otherwise by manufacturer or by HCIS.

This includes HVAC systems for facilities housing security equipment.

نسخة من خطة شركة المياه الوطنية

5.11.1.6. The actual PM performed shall be documented and be available for review for at least one calendar year. During PM the performance of all the components shall be validated to perform to its design requirements. Both the FO or his representative and the contractor's signature shall be on the PM sheet declaring satisfactory execution of PM.

5.11.1.7. The FO shall have a facility, manned 24 hours a day, 7 days a week, available for field personnel to report failures via telephone, radio or security system telemetry.

5.11.1.8. FO shall be responsible for classifying system failures as critical or non-critical failures.

5.11.1.9. Critical failures shall be rectified within 8 hours of failure report.

5.11.1.10. Non-critical failures shall be rectified within 48 hours.

5.11.1.11. FO shall develop and maintain a proper recording/tracking system for all failures reported to the applicable contractor.

5.11.1.12. System failures and alarms shall be analyzed quarterly by the FO to identify potential problem areas. This quarterly review shall be used as the basis for the development of strategies to rectify the problems identified.

5.11.1.13. The FO shall maintain documentation for all security equipment installed. This documentation shall include full contact details of component manufacturers, part numbers, recommended spare parts and maintenance manuals needed for each security installation.

5.11.1.14. The FO shall maintain a full set of As Built drawings for all security systems and civil work. The drawings shall be maintained as soft copy in an easily accessible format. The FO shall maintain an index of all drawings pertaining to all security related work. All drawings shall be stored in a secure location and in a secure format.

5.11.2. Fences

FO shall implement a fence and fence line maintenance program to ensure the fence and entire fencing system area is kept in acceptable condition.

5.11.2.1. Monthly

- The fences shall be checked monthly and cleared of all accumulated debris such as plastic bags that are adhering to the fences.
- Any plant growth in excess of 155mm height above grade shall be cleared from all areas of the fence and fence area.

5.11.2.2. Quarterly

- Any sand accumulation around the fences and fence line shall be cleared to ensure that the height from grade to the top of the fence is maintained at 3m.
- In cases of severe sand accumulation the FO shall implement a sand removal program at shorter intervals.
- MARINE AREAS ONLY: The fence shall be inspected to ensure all structural and installation components are in good condition and free from corrosion.

5.11.2.3. Yearly

- All clear zones and fence areas shall be checked and graded to maintain grade as specified in SEC-02.
- All clear zones and fence areas shall be cleared of all vegetation.
- The fence shall be inspected to ensure all structural and installation components are in good condition and free from corrosion.

نسخة مرخصة لشركة المياه الوطنية

5.11.3. Emergency Power Generator

All emergency generators installed for directive compliance shall be tested by the FO on the following schedule:

5.11.3.1. Weekly startup test, fluid level check and fuel tank top off.

5.11.3.2. Monthly full load test and power transfer switch test.

5.11.3.3. Monthly tests shall be performed to confirm the ability of the alternate power feed to carry the full load.

5.11.3.4. Emergency power supply components shall be maintained and tested as mandated by NFPA 110.

5.11.3.5. Any problems detected during the testing shall be rectified within 24 hours.

5.11.4. Uninterruptible Power Supply

All UPS's shall be tested at manufacturer recommended intervals, or the intervals listed below, whichever is shorter:

5.11.4.1. 3 Months

- Visually inspect equipment for loose connections, burned insulation or any other signs of wear.
- Test UPS transfer switches, circuit breakers and maintenance bypasses.

5.11.4.2. 6 Months

- Visually check for liquid contamination from batteries and capacitors.
- Clean and vacuum UPS equipment enclosures.
- Check HVAC equipment and performance related to temperature and humidity.

5.11.4.3. 12 Months

- Check all electrical connections to ensure all are tight and not generating heat, which is the first and sometimes only indication of a problem. Diagnostic tools may help technicians identify hot spots invisible to the human eye. Technicians should re-torque if evidence of a loose connection is found.
- Provide a complete operational test of the system, including a monitored battery-rundown test to determine if any battery strings or cells are near the end of their useful lives.

Any problems detected during the testing shall be rectified within 24 hours.

5.11.5. Lighting System

FO shall implement a maintenance program to detect and replace failed lamps or lighting system devices within 72 hours of detection.

If adjacent luminaires or luminaires used for perimeter lighting fail, at least one of them shall be repaired within 24 hours.

FO shall ensure that all devices and materials needed for lighting system maintenance and support are available at the facility. This includes spare parts, ladders, lifts and cleaning materials.

5.11.5.1. Lamp Lumen Depreciation

Lamps used for security lighting have a limited life that is specified by manufacturers Lamp Lumen Depreciation (LLD) parameter.

- FO shall implement a luminaire group re-lamping program based on the LLD parameter.
- Lamps shall be replaced when they reach between 70% - 80% of the estimated life.
- FO shall maintain a maintenance log for lamp replacement in each luminaire.

5.11.5.2. Luminaire Dirt Depreciation

Luminaires are characterized by manufacturer's Luminaire Dirt Depreciation (LDD) parameter which gives a measure of how fast the luminaire will accumulate dirt that will effectively reduce light output.

- FO shall implement a luminaire cleaning program based on the manufacturers LDD parameter.
- Luminaire cleaning shall be carried out as specified by the luminaire LDD parameter or every 24 months, whichever is shorter.
- More frequent cleaning shall be performed for facilities located in areas prone to dirt accumulation on the luminaire.

5.11.6. Security Devices

Surveillance Cameras

All surveillance cameras shall have their lenses cleaned when the image shows signs of degradation due to accumulations on the lenses or at the intervals listed below, whichever is shorter:

5.11.6.1. 3 Months

- Clean camera lenses with approved lens cleaning methods and materials.
- Surveillance cameras in marine areas may require more frequent cleaning due to salt spray accumulation.

5.11.6.2. 6 Months

- Visually inspect camera housing and conduits for damage or corrosion.
- Ensure camera housings and fittings are secured.

Explosive Trace Detectors (ETD)

5.11.6.3. 3 Months

Operational ETD's shall be tested according to the procedures specified in ASTM E2520-07.

5.11.6.4. 6 Months

Operational ETD's shall be tested for performance and the results shall be documented and retained for an 18 month period. A probability of detection of 75% shall be acceptable for performance verification testing.

X-Ray Systems

5.11.6.5. FO shall daily use an ASTM F792-08 compliant test target to verify X-ray performance. The results of the test shall be documented, as per ASTM F792, and retained for 3 months.

5.11.6.6. The X-ray units shall be repaired with parts certified by the manufacturer. Substitute parts shall only be used if approved by the manufacturer.

5.11.6.7. X-Ray unit repairs shall be documented and made available to HCIS when requested.

5.11.6.8. In case a repair operation is carried out or the unit is moved, the unit shall not be returned to operation until a radiation survey certifies that radiation emitted from the X-ray unit cabinet shall not exceed 0.5 milliroentgen in one hour at any point five centimeters outside the cabinet.

5.11.6.9. General

FO shall ensure that all security devices and infrastructure are maintained at manufacturer specified intervals. Such maintenance shall include daily user inspection and maintenance staff preventive maintenance.

These maintenance activities shall be included in the maintenance plan and documented.

5.12. Safe Work Practices

The FO shall integrate safe work practices into all aspects of security operations, procedures and post orders.

5.13. Management of Change

FO shall put in place a process to manage the changes in the security posture with due consideration to the following:

5.13.1. Security-related countermeasures.

5.13.2. Target assets.

5.13.3. Vulnerability status of the site.

5.13.4. Threat environment affecting the site.

5.13.5. Key security-related policies, procedures, or practices.

5.13.6. Process, system, equipment, inventory, or other aspect of the site that in any way alters the results, conclusions, or recommendations of the facility specific SRA.

5.13.7. Audit and reporting system.

نسخة مرخصة لشركة البيان الوطنية

5.14. Incident Reporting & Investigation

Security Incidents at the facilities shall be investigated and corrective actions shall be taken to prevent recurrence:

5.14.1. All security incidents at a facility shall be documented and retained for an 18 month period. The documentation shall be available for review by HCIS.

5.14.2. The FO shall conduct periodic audits of all security equipment to review status and uptime.

5.15. Emergency Planning

The FOs shall have an emergency management plan in place to help contain and mitigate the consequences of actual or imminent occurrence of malicious acts.

FO shall ensure that all ISD personnel are familiar and trained in their responsibilities under the facility emergency response plan and the specific security emergency procedures as stipulated in section 5.4.4 above.

Emergency Planning shall comply with SAF-20: Pre-Incident Planning and Management of Emergencies and shall include security scenarios.

5.16. Compliance Audits

The FOs shall conduct annual self-assessment of compliance with SEC directives, identify gaps and develop a plan for corrective actions.

نسخة مرخصة لـ [illegible]

6. Application of Requirements

This section list show the elements of this security directive apply to facilities depending on their FSC.

REQUIREMENT	Facility Security Classification (FSC)				
	1	2	3	4	5
Accountability	✓	✓	✓	✓	
Risk Assessment & Management	✓	✓	✓	✓	
Standing Operating Procedures	✓	✓	✓	✓	✓
Facility Security Plan	✓	✓	✓	✓	
IS Department	✓	✓	✓	✓	
Construction, Commissioning & Startup	✓	✓	✓	✓	
Personnel Management	✓	✓	✓	✓	
Competency & Training	✓	✓	✓	✓	
Weapons Control	✓	✓	✓	✓	
Transportation	✓	✓	✓	✓	
Maintenance & Support	✓	✓	✓	✓	✓
Safe Work Practices	✓	✓	✓	✓	✓
Management of Change	✓	✓	✓	✓	
Incident Reporting and Investigations	✓	✓	✓	✓	✓
Emergency Planning	✓	✓	✓	✓	✓
Compliance Audits	✓	✓	✓	✓	✓

نسخة من هيئة شبكة المياه الوطنية

7. Proof of Compliance

New & Upgrade Projects

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items. The Stage 3 submission, content and format are specified in SEC-14 section 6.3. This PoC shall form part of Section 3 of the Stage 3 submission package.

Existing Facilities

This PoC shall provide details for each of the requirements listed below on the four year SRA cycle. All changes, if any, from the previous submission shall be clearly identified.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-15 Reference	Requirement	FO Response
1.	5.2	Security Risk Assessment Management	*Provide a copy of the SRA*
2.	5.3	Facility Security Plan	*Provide a copy of the FSP*
3.	5.4	Standing Operating Procedures	*Provide a copy of the SOP's*
4.	5.6	Construction, commissioning & Start-up	*Provide a certificate that all aspects in section 5.6.3 has been completed with relevant documentation in place*
5.	5.8	Competency & Training of Security Personnel	*Provide list of training courses that are being provided* *List the number of personnel trained in each of these courses*
6.	5.11	Maintenance & Support program	*Provide copy of annual Maintenance & Support program* *List summary and statistics on annual activity*
7.	5.16	Compliance Audits	*Provide copy of annual Compliance Audit results with correction plan*

APPENDIX-A: Typical Security Management Documentation

1. Security Management Policy
2. Security Plan
3. Security Personnel
   - 3.1 Responsibilities
   - 3.2 Job Description
     - 3.2.1 Superintendent Industrial Security
     - 3.2.2 Security Supervisor
     - 3.2.3 Security Shift Captain
     - 3.2.4 Security Man
   - 3.3 Post Orders
     - 3.3.1 General Instructions
     - 3.3.2 Security Shift Captain
     - 3.3.3 Gate Security Man
     - 3.3.4 Security Patrol Man
     - 3.3.5 CCTV Operator
     - 3.3.6 Visitor/Reception Security Man
     - 3.3.7 Security Control Centre Operator
     - 3.3.8 X-Ray Checkpoint Security Man
     - 3.3.9 Foot Patrolling
     - 3.3.10 Mobile Patrolling
     - 3.3.11 Security Man Turnstile Gate
     - 3.3.12 Security Man Material Department Gate
     - 3.3.13 Security Man Admin Building Reception
4. Security Procedures
   - 4.1 Physical Security
     - 4.1.1 Access Control
     - 4.1.2 IS Card Procedures
     - 4.1.3 Visitors
     - 4.1.4 Vehicle Entry Permit
     - 4.1.5 Material Control
     - 4.1.6 Key Control
   - 4.2 Information Security
     - 4.2.1 Document Security
     - 4.2.2 Photography Permit
     - 4.2.3 Laptop Computer Permit

نسخة مرخصة لشركة [illegible]

4.3 Security Training (example Formal, Refresher, Equipment, On the Job etc)
4.4 Security Management
- 4.4.1 Daily Security Reports
- 4.4.2 Security Statistics and Performance Measurement
- 4.4.3 Security Incident Report
- 4.4.4 Uniforms for Security Staff
- 4.4.5 Maintenance of Security Systems and Equipment
- 4.4.6 Handling and Storage of Weapons
- 4.4.7 Communication with Security Services Contractors and Suppliers
- 4.4.8 Waiving of Standard Security Procedures

4.5 Specific Security Incidents
- 4.5.1 Emergency Response
- 4.5.2 Bomb Threat
- 4.5.3 Dealing with suspicious parcels
- 4.5.4 Lost and Found Items
- 4.5.5 Vehicle Accidents
- 4.5.6 Workplace Violence
- 4.5.7 Security Alert Levels
- 4.5.8 Security Breaches – Illegal document copying/removals etc.

4.6 Industrial Security Department Forms
- 4.6.1 ISD-01 Visitor's Application Form
- 4.6.2 ISD-02 Departmental Authorized Signatory Form
- 4.6.3 ISD-03 Request for ID Card Form
- 4.6.4 ISD-04 Temporary Entry Permit Form
- 4.6.5 ISD-05 Reporting Loss of ID Card Form
- 4.6.6 ISD-06 Vehicle Entry Permit Application Form
- 4.6.7 ISD-07 Material & Equipment Gate Pass
- 4.6.8 ISD-08 Security Post Report
- 4.6.9 ISD-09 Shift Report
- 4.6.10 ISD-10 Daily Security Report Form
- 4.6.11 ISD-11 Security Incident Report Form
- 4.6.12 ISD-12 Bomb Threat Information Form
- 4.6.13 Equipment/Waste removal permit – Permanent transfer/Dispose/Repair –Return.

نسخة مرخصة لشركة الهيل الوطنية

APPENDIX-B: Security Risk Assessment

1.0. Introduction

A Security Risk Assessment (SRA) is the process that quantifies the risk of security events, determines the countermeasures required and the differential between existing countermeasures and what is needed.

1.1. Facility Operators (FO) shall review the facility by conducting an SRA as specified below:

1.1.1. An initial assessment of the facilities to determine FSC and formulate the baseline for the FSP development.

1.1.2. When the commissioning of a new facility is completed an SRA shall be conducted as follows:

- For Class 1 facilities 1 per year with a follow-up meeting.
- For Class 2 facilities 1 per year.
- For Class 3 & 4 facilities 1 every 18 months.

1.1.3. When a new process or operation is proposed, and prior to implementation. This includes the expansion of existing facilities or any change in the physical layout of the facility.

1.1.4. When the threat substantially changes, at the discretion of the security manager of the facility or when directed by HCIS.

1.1.5. After a significant security incident.

1.2. The SRA shall be conducted by a qualified security consultant as described below in section 2, 3 & 4.

1.3. The SRA shall be submitted for HCIS review and approval as stipulated in SEC-15 section 5.2 and for “projects” as stipulated in SEC-14 section 6.1.

2.0. Methodology

2.1. The SRA shall be conducted by utilizing any of the SRA methodologies or standards as described in the following:

- ANSI/API Standard 780 – *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*, First Edition, March 2013.
- CCPS *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*.
- ASIS International *Risk Assessment Standard* ANSI/ASIS/RIMS RA.1-2015

2.2. The SRA shall consider and include each of the five steps of the API / CCPS /ASIS methodologies.

2.3. The SRA shall include and consider the following, as a minimum but not limited to, for analysis and determining the facility characterization:

2.3.1. Description of the facility layout and infrastructure.
2.3.2. Result of the Business Criteria Analysis (BCA).
2.3.3. Results of the Process Hazard Analysis (PHA), as defined in SAF-02, which includes operational processes analysis.
2.3.4. Existing security infrastructure and physical security measures.
2.3.5. Existing security organization and personnel.
2.3.6. Security Plan, Procedures & Post Orders.

2.4. The content of the SRA shall be explained and illustrated with legible drawings of the facility layout with annotated photos of all existing security infrastructure & countermeasures. (See Section 3 below for detail).

2.5. For an existing facility, the SRA shall clearly identify all the areas of non-compliance with HCIS SEC Directives for the recommended FSC of the facility.

2.6. The SRA shall include recommended security countermeasures and upgrading required for achieving full compliance with the SEC Directives as stipulated for the specific FSC of the facility.

2.7. The SRA countermeasure recommendations shall be grouped into the following sections:

2.7.1. Facility Security Classification
2.7.2. Security Organizational/personnel measures
2.7.3. Security Procedural measures
2.7.4. Physical (including Technical) Security measures

2.8. The recommendations shall be site specific and in much detail to be translated into the FSP design. Generalized generic statements, such as “Install HCIS Class 1 fencing” shall be avoided. Recommendations shall include specifically what must be done/required and where.

2.9. Recommendations shall be based on the preceding analysis in the SRA and based on the principle of “security in depth” and a strategy of Deter, Detect, Delay, Respond and Recover.

2.10. The Facility Security Classification shall be based on the analysis of the Business Criteria Analysis, Process Hazard Analysis and Risk Evaluation in the SRA.

2.11. Organizational/personnel recommendations will form the basis for the size of the security organization, identification of security posts and staffing, as well as the training requirements for security personnel and employees.

2.12. Procedural recommendations will provide the basis for the documentation (Security Policy & Plan, Security Procedures and Post Orders) required in the execution of the security function and the integration of physical security countermeasures with the security personnel performing the tasks.

2.13. Physical Security measures/recommendations form the basis for the physical security system design and specify the physical security infrastructure and technical equipment required to protect the facility and critical assets.

2.14. The physical security recommendations shall include the following as a minimum:

2.14.1. The physical security measures required to comply with the recommended FSC.
2.14.2. Facility perimeter and perimeter requirements.
2.14.3. Internal separation fencing as required.
2.14.4. Security lighting (perimeter, area, check point and specific critical areas and buildings).
2.14.5. Gates and access points into the facility with the specific requirements for each gate.
2.14.6. Perimeter Intrusion Detection, Surveillance & Assessment requirements.
2.14.7. Protection of Critical Assets, buildings and specific areas in the facility.
2.14.8. Electronic Access Control measures.
2.14.9. Communication and emergency communication.

2.15. The SRA shall clearly identify all areas where compliance with HCIS SEC Directive requirements cannot be achieved with recommendations on how this non-compliance will be mitigated.

2.16. Where applicable, the SRA shall clearly identify the risks associated with the land/water interface of facilities located on the coast and provide specific recommendations for the protection of the facility and the integration with

other stakeholders such as the Coast Guard. This includes facilities with piers, a jetty, seawater intake, or other marine facilities.

2.17. The FO shall use the Organizational recommendations from the SRA to develop the Security Organization, determine the number of security personnel and formulate the training program & requirements.

2.18. The FO shall use the Procedural recommendations to formulate the Security Plan, Procedures & Post Orders for the facility (Security Manual).

2.19. The Security Consultant shall use the Physical security recommendations to develop a conceptual design for the physical security system & infrastructure.

2.20. The aim of the SRA recommendations is not to identify the FSC with associated requirements or to satisfy HCIS but to provide a basis for the security program at the facility based on the principle "*security in depth*".

3.0. SRA Submittal Content for HCIS Review

3.1. The SRA shall be submitted and presented to HCIS in folders, clearly marked as specified in SEC-14 section 6.1.

3.2. Documentation for HCIS review shall be separated, grouped and marked in Parts (the folder) and Sections (within the folder) as indicated in sections below.

3.3. Any SRA submittal for HCIS review shall consist of three Parts.

3.3.1. PART 1 – The SRA document with recommendations and attachments.

3.3.2. PART 2 - The implementation Plan for all the SRA physical security countermeasure recommendations. SRA's conducted for "Greenfield" projects or expansion projects at existing facilities shall include the Concept of Design (COD) as described in SEC-14 section 6.1.2.

3.3.3. PART 3 - The implementation plan for the SRA recommendations for the Security Organization, Policy & Procedures, and Training as described below.

3.4. PART 1: Security Risk Assessment

The SRA ring binder shall contain the following documents as indicated:

3.4.1. Section 1. The SRA document.

3.4.2. Section 2. All drawings required and referenced in the SRA. The following minimum shall be included:

3.4.2.1 A drawing of legible size to clearly indicate the facility location, all adjacent facilities and infrastructure bordering the facility.

3.4.2.2 A detailed plot plan of the facility clearly identifying the facility perimeter, all access points/gates, internal and external roads and main infrastructure.

3.4.2.3 A drawing indicating the various assets identified in the SRA. Drawings should include piers, seawater intakes, marine facilities, railway tracks as applicable.

3.4.2.4 All drawings shall be annotated, assets and infrastructure clearly marked and numbered with a legible legend on the drawing.

3.4.3. Section 3. The Business Impact Analysis shall be attached as references and supporting documentation for the assessment of the FSC.

3.4.4. All appendixes and documentation submitted with the SRA shall be referenced in the content and text of the SRA.

3.5 PART 2. Implementation Plan for SRA Physical Security Recommendations

3.5.1 Part 2 contains the implementation plan of the Facility Security Classification (FSC) and Physical Security Countermeasure Recommendations made in the SRA.

3.5.1.1 The Security Consultant shall prepare a Conceptual Design (COD) as stipulated in SEC-14 section 6.1.2 and incorporate the FSC, physical security measures as the proposed implementation plan for the recommendations.

3.5.1.2 Any SRA submitted to HCIS which are not done for a green field project or expansion project shall include a time table prepared by the FO for the implementation of the SRA recommendations.

Section 1: 10% Conceptual Design Document or the Implementation Plan for the SRA Physical Security Countermeasure Recommendations.

Section 2: Site specific drawings covering items & related equipment listed in SEC-14 section 5.6.

Section 3: Summary of Waiver request with justification for each non-compliance of HCIS Security Directives (If applicable) as identified in the SRA. Detailed Waiver requests shall be included in the Stage 2 submittal.

3.6 PART 3. Implementation plan for the Security Procedural and Security Organizational/personnel recommendations.

3.6.1 The conceptual implementation plan shall consist of the following sections:

Section 1: Procedural measures. The FO shall include the implementation plan for all the recommendations under this section, such as:

- List of existing Security Procedures and new procedures required.
- A plan for the revision & updating of the existing Security Procedures.
- List of existing Post orders and new Post Orders required.
- A plan for the revision & updating of the existing Post orders.
- Facility security infrastructure and equipment Maintenance Plan.

Section 2: Organizational/Personnel measures. The FO shall include the implementation plan for all the recommendations under this section, such as a proposed security organization, security personnel required, security training program, summary of required job descriptions, etc.

3.6.2 The Implementation Plan for "Green Field" projects shall include the following documentation:

3.6.2.1 Documentation as stipulated in section 3.5.1.1 & 3.5.1.2 prepared by the security consultant.

3.6.2.2 A proposed "Table of Contents" for the Security Manual (Facility Security Plan, Procedures & Post Orders) and training to be conducted as derived from the SRA (with specific reference to sections 2.7.2 & 2.7.3 above).

The FO shall develop the listed Security Plan, Security Procedures & Post Orders (Security Manual) as part of the project documentation.

3.6.2.3 The concept Security Manual shall be submitted to HCIS as part of Stage 3 submittal as stipulated in SEC-14 section 6.3.1.

3.6.2.4 The final version of the Security Manual, Security organizational documentation (Organization Chart, Security Staff Training, etc.) and security infrastructure and equipment Maintenance Plan shall be completed prior to Stage 4 and available for HCIS review during the Operational Readiness Inspection as described in SEC-14 section 6.4.1.

3.6.3 The FO shall implement a tracking system to ensure that the "Organizational" & "Procedural measures" are developed simultaneously and progress status reported/submitted throughout all the stages as specified in SEC-14.

4.0. SRA Format

The FO may use any of the three methodologies listed in section 2.1 above to conduct the SRA so long as the process is consistent with the five (5) steps of the API Standard 780, First Version, 2013 methodology, and the end result meets the same objective.

At completion of each step the FO shall summarize the analysis of information and data during the particular step under a specific heading "conclusions" for each step. The conclusions after each step shall provide the basis for the SRA Recommendations as a final step in the SRA process.

Regardless the various steps of the specific methodology, all steps shall be grouped under the following headings which forms the layout and format of the SRA:

- Facility & Asset Characterization
- Threat Assessment
- Vulnerability Assessment
- Risk Assessment
- SRA Recommendations

4.1 Facility & Asset Characterization

This step shall follow the analysis of the specific methodology but include the following additional elements:

4.1.1 Detailed description and analysis of the facility layout and all elements as described in section 2.3 above.
4.1.2 Condition of the existing security infrastructure, perimeter and perimeter layout, number of entrance gates, their location, role and function of each gate and impact on facility operation.
4.1.3 Internal separation fences & gates and impact on facility operation.
4.1.4 Conclusion on assets and critical areas to be protected
4.1.5 Conclusion on existing security organization, manpower & training.
4.1.6 Conclusion on existing security program, procedures & post orders.

4.2 Threat Assessment

This step shall follow the analysis of the specific methodology but include the following additional elements:

4.2.1 Conclusion on the identified potential threats to the facility and specific assets.
4.2.2 Conclusions on the impact of identified potential threats on existing security countermeasures (infrastructure, organization, procedures).

4.3 Vulnerability Assessment

This step shall follow the analysis of the specific methodology but include the following additional elements:

4.3.1 Conclusions on the possible consequence and vulnerability of identified potential threats on assets and facility infrastructure.
4.3.2 Conclusions from ranking the severity of consequence on assets and facility infrastructure.

4.3.3 Where the facility relates to water the FO shall ensure that security of the following specific water facility elements are addressed:

- Open reservoirs
- Covered reservoirs
- Air vents
- Reservoir inlets/outlets
- Access hatches
- Sample taps
- Pressure monitoring devices
- SCADA system components
- Disinfection systems
- Chemical storage facilities
- Chemical injection systems
- Pump Stations
- Hydrants
- Blow-offs
- Air valves
- Main valves
- Backflow devices

4.4 Risk Assessment

This step shall follow the analysis of the specific methodology with specific conclusions from the risk evaluation and risk-ranking which will form the basis for the SRA recommendation ns.

4.5 SRA Recommendations

The final step or heading of the SRA shall be SRA Recommendations which is a summary of the Countermeasure Analysis or Risk Treatment.

4.5.1 The recommendations shall be site specific, not generic, and provide clear security requirements for the development of the physical security conceptual design (COD), the security organization and the security procedures.

All recommendations shall be prioritized and grouped into Organizational, Procedural, Physical and Technical categories.

نسخة من خصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-16

Pipelines & Pipeline Corridors

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Version 1.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7
2 SCOPE 7
3 ACRONYMS & DEFINITIONS 7
4 REFERENCES 7
5 GENERAL REQUIREMENTS 8
5.1. Related Directives 8
5.2. Security Risk Assessment 8
5.3. Ownership 9
5.4. Fence Penetrations 9
5.5. Patrols 9
5.6. Response Plan 9
5.7. Urban Areas 9
5.8. Maintenance of Pipelines & Pipeline Corridors 9
6 PROOF OF COMPLIANCE 10

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document provides security requirements for pipelines and pipeline corridors used by industrial facilities under the jurisdiction of HCIS.

2 Scope

This directive specify the minimum requirements needed for the protection of pipelines and pipeline corridors.

3 Acronyms & Definitions

FO	Facility Operator The owner, operator or lessee of a facility
HCIS	High Commission for Industrial Security
ROW	Right of Way
SAF	Safety and Fire Protection Directives
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory recommendation
SRA	Security Risk Analysis

4 References

This directive adopts the latest edition of the references listed.

The selection of material and equipment, and the design, construction, maintenance, operation and repair of equipment and facilities covered by this Security Directive shall comply with the latest edition of the references listed in each Security Directive, unless otherwise noted.

ACI 318-05	*Building Code Requirement for Structural Concrete*
SAF-10	*Pressure Piping, Transportation Pipelines and Pressure Vessels*
SEC-01	*General Requirements for Industrial Security*
SEC-02	*Security Fencing*
SEC-05	*Security Systems at Industrial Facilities*
SEC-18	*Industrial Cities*

نسخة غير خاصة بشركة المياه الوطنية

5 General Requirements

Pipelines, for the purpose of this directive, are defined as those pipelines that are exposed and external to a facility and convey material to/from an industrial facility, or natural source, to a delivery point for either sale, export, consumer use or as part of a manufacturing process.

A pipeline corridor or right-of-way (ROW) is a strip of land over and around pipelines where a pipeline operator may install or maintain pipeline with the permission and requirements of the owner of the pipeline corridor. Multiple pipelines conveying multiple products may utilize the corridor and each pipeline may terminate at different locations.

In all cases, pumping stations, pipeline scrapers, valves etc. shall be considered as part of the pipeline and its infrastructure.

5.1. Related Directives

Pipeline design and installation shall comply with the requirements of the following related directives:

1. SAF 10: Pressure Piping, Pressure Vessels & Transportation Pipelines
2. SEC-18: Industrial Cities

In general, FO shall comply with all SEC and SAF requirements.

5.2. Security Risk Assessment

The basis of specifying the protection of pipelines shall be a Security Risk Assessment (SRA) carried out by an HCIS approved Security Consultant. SRA requirements are specified in SEC-01.

SAF-10 specifies safety requirements for the pipeline. The SRA shall consider these requirements when recommending security measures to protect the pipeline and associated critical infrastructure. Critical areas, such as but not limited to, pump stations, scraper launcher or receivers and isolated valve stations, shall be specifically protected according to SRA recommendations.

The SRA shall be carried out for existing pipelines and new pipelines.

5.3. Ownership

The FO shall determine the ownership and responsibilities for pipelines and pipeline corridors based on:

- The unique purpose and operation of the pipeline/pipeline corridor.
- The type of product transported by the particular pipeline/pipeline corridor.
- The security, operations and maintenance services to be performed along the entire pipeline/pipeline corridor.

5.4. Fence Penetrations

Single pipeline penetration shall adhere to the requirements as stipulated in SEC 02 and pipeline corridor penetration shall adhere to requirements stipulated in SEC 19. In both cases, the SRA shall determine fence penetration measures.

5.5. Patrols

FO shall ensure that critical pipelines are regularly patrolled along their entire length. Patrols may be implemented using direct view by security personnel or imaging systems that have adequate resolution to detect intruders in the pipeline ROW.

The required patrols and their frequency and the technology used for patrol implementation shall be determined by the SRA recommendations.

5.6. Response Plan

FO shall implement a response plan to respond to events along the pipeline. FO shall ensure that the response plan shall be coordinated and managed.

5.7. Urban Areas

Pipelines and ROW's in urban, built up areas shall be fenced off and have surveillance systems installed in those sections. Surveillance systems shall be monitored at the FO SCC. The SRA shall determine the extent and location of the fencing.

5.8. Maintenance of Pipelines & Pipeline Corridors

The immediate area next to and under the pipeline shall be kept clean of vegetation. A minimum clear zone of 3m shall be maintained on both sides.

6 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-16 Reference	Requirement	FO Response
1.	5.1-2 & 5.4	Fence Penetration	*Provide drawing with dimensions showing fence penetrations*
2.	5.2	SRA	*Provide SRA*
3.	5.3	Ownership	*Provide FO/Company name responsible for pipeline/pipeline corridor*
4.	5.5	Patrols	*Provide data on patrol frequencies and methods*
5.	5.6	Response Plan	*Provide response plan*

نسخة من خطة المملكة لحماية المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-17

Electrical Power Substations

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Version 1.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7
2 SCOPE 7
3 ACRONYMS & DEFINITIONS 7
4 REFERENCES 7
5 GENERAL REQUIREMENTS 8
5.1. INTRODUCTION 8
5.2. TYPICAL SECURITY REQUIREMENTS 8
5.3. HCIS APPROVAL STAGES 9
5.4. FC BASIS 9
5.5. FC CRITERIA 9
5.11. FC BCA WORKSHEET 12
6 PROOF OF COMPLIANCE 15

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

The purpose of this document is to provide a method for classifying electrical substations to establish security requirements.

2 Scope

This standard details security requirements at all electrical power sub-stations within Saudi Arabia.

3 Acronyms & Definitions

BCA	Business Criteria Analysis
CNI	Critical National Infrastructure
FC	Functional Classification
FO	Facility Operator: the owner, operator or lessee of a facility
FSC	Facility Security Classification
OCF	Operations Control Facility
SCC	Security Control Center:
SEC	Security Directives
Shall	Indicates a mandatory requirement
Should	Indicates an advisory requirement
SRA	Security Risk Assessment
TSR	Typical Security Requirement

4 References

SEC-01–SEC-19	All Security Directives

نسخة من نص الهيئة الوطنية

5 General Requirements

5.1. Introduction

Electrical substations present a special case and cannot be classified into any of the existing High Commission for Industrial Security (HCIS) Facility Security Classifications (FSC) for industrial facilities as stipulated in SEC-01 section 8.

This document addresses the specific requirements of substations and provides criteria for determining their Functional Classification (FC) and the security requirements, based on existing Security Directives, for each FC.

The requirements for each security system, sub-system and component shall comply with the requirements of HCIS SEC 01 - 19. Where directive requirements cannot be complied with due to space constraints, or other valid reasons, then a waiver may be submitted as specified in SEC-01.

5.2. Typical Security Requirements

Most substations are typical in design in terms of loads and limited space availability. FO may submit typical annual security requirements for each substation FC. This Typical Security Requirements (TSR) document shall be submitted in the third quarter (3Q) of every calendar year for utilization in the following calendar year.

The TSR provides a general approach to security design for similar substations. It does not address site specific requirements as noted below:

5.2.1. FO shall note that for facilities located in border areas, or due to HCIS request, security requirements may be increased at any time over the baselines defined in the TSR document.

5.2.2. Site specific waivers shall be applied for where applicable during the design stage and prior to initiation of construction.

5.2.3. General waivers for all sites may be applied for in the TSR for any calendar year.

5.3. HCIS Approval Stages

The HCIS approval stages specified in SEC-01, section 12.2, shall be amended as follows for electrical substations:

5.3.1. Electrical substations at industrial facilities classified as Class 1, 2 or 3 shall continue to follow the standard HCIS approval stages.

5.3.2. Electrical substations at all other locations shall utilize the approved TSR as the basis for security design and implementation. The TSR shall be approved for the calendar year in which construction is initiated for the specific site.

5.4. FC Basis

Substations shall be functionally classified by conducting a Business Criteria Analysis (BCA) and the risks determined by the Security Risk Assessment (SRA) as stipulated in SEC-01 section 8.3. Once the FC has been established, the corresponding security requirements stated in this document shall be designed and implemented for each substation location.

FO shall note that specific considerations applicable to electrical substations may be incorporated into the SRA methodology to comprehensively address all facility specific risks associated with its design and function.

5.5. FC Criteria

Each electrical substation shall have a Functional Classification (FC) assigned based on the Business Criteria Analysis (BCA), and the risks determined by the Security Risk Assessment (SRA).

FO shall submit a recommended FC to HCIS for approval. HCIS reserves the exclusive right to amend the final FC for a substation.

Substations shall be classified based on a five (5) level classification methodology with Class A being the highest level and Class E being the lowest level.

The business criteria for determining the FC of a specific facility are defined in the sections below.

5.6. **Class A Substation**

A Class A substation is a critical element in the power network.

Business Criteria

Such a substation is characterized by meeting ANY of the following criteria:

5.6.1.1. Directly and seriously impacts hydrocarbon exports.
5.6.1.2. It will affect Critical National Infrastructure in case of loss.
5.6.1.3. Critical element in supporting electrical grid capacity.
5.6.1.4. Loss of function/capacity cannot be compensated for by another substation within 12 hours for critical loads.
5.6.1.5. Loss of function/capacity would result in more than 75% reduction in supply capacity in its service area.
5.6.1.6. Full time operational staff on site.
5.6.1.7. Contains a grid Operations Control Facility.

Security Requirements Overview

A Class A substation shall comply with the following security requirements:

5.6.1.8. SEC-01 through SEC-19 requirements for a Class 1 facility.
5.6.1.9. Full time Industrial Security Staff onsite.
5.6.1.10. Local Security monitoring as specified in SEC-05, section 5.11.

5.7. **Class B Substation**

A Class B substation is a very important element in the power network.

Business Criteria

Such a substation is characterized by meeting ANY of the following criteria:

5.7.1.1. Directly impacts hydrocarbon exports, but will not significantly reduce them.
5.7.1.2. Minor impact on Critical National Infrastructure in case of loss.
5.7.1.3. Very important element in supporting electrical grid capacity.
5.7.1.4. Loss of function/capacity cannot be compensated for by another substation within 24 hours for critical loads.
5.7.1.5. Loss of function/capacity would result in more than 50% of reduction in supply capacity in its service area.

Security Requirements Overview

A Class B substation shall comply with the following security requirements:

5.7.1.6. SEC-01 through SEC-19 requirements for a Class 2 facility.
5.7.1.7. Full time Industrial Security Staff on site.
5.7.1.8. Locally monitored at gatehouse.

5.8. Class C Substation

A Class C substation is an important element in the power network.

Business Criteria

Such a substation is characterized by meeting ANY of the following criteria:

5.8.1.1. An important element in supporting the electrical grid capacity.
5.8.1.2. Loss of function/capacity cannot be compensated for by other substations.
5.8.1.3. Loss of function/capacity would result in more than 25% reduction in supply capacity in its service area.

Security Requirements Overview

A Class C substation shall comply with the following security requirements:

5.8.1.4. SEC-01 through SEC-19 requirements for a Class 3 facility.
5.8.1.5. No permanent Industrial Security Staff required on site.
5.8.1.6. Industrial Security and/or Government Security Forces conduct regular patrols.

5.9. Class D Substation

A Class D substation is a less important element in the power network.

Business Criteria

Such a substation is characterized by meeting ANY of the following criteria:

5.9.1.1. Loss of function/capacity would result in more than 15% reduction in network capacity.
5.9.1.2. Remote support facility to other substations.

Security Requirements Overview

A Class D substation shall comply with the following security requirements:

5.9.1.3. SEC-01 through SEC-19 requirements for a Class 4 facility.

5.9.1.4. No permanent Industrial Security Staff required on site.

5.9.1.5. Industrial Security and / or Government Security Forces conduct regular patrols.

5.10. **Class E Substation**

A Class E substation is a local distribution substation and feeds residential loads, commercial loads, a single facility or sections of a facility.

Business Criteria

5.10.1.1. The design of this substation consists of standalone building/buildings located in residential/commercial areas, within or near facilities/compounds.

5.10.1.2. Security countermeasures for these substations are dependent on its location which should be evaluated during the TSR/SRA process.

5.11. FC BCA Worksheet

Electric substation owners, operators or lessees shall provide HCIS with details that are considered as part of the Functional Classification (FC).

A typical worksheet shown on the next page shows the type of information that is required to develop the FC. The data from the worksheet shall be provided to HCIS as part of the SRA.

HCIS shall evaluate this data, and the recommended FC, and provide the applicant with approvals or revisions for the FC.

Security configurations for each substation shall be based on the FC. The criteria for developing the FC are shown on the following pages.

	Substation Name:		
	Location:		
	Criteria	Yes/No	Details
	Class A		
1.	Directly & seriously impacts hydrocarbon exports	Y/N	*List critical hydrocarbon facilities supplied from this substation*
2.	Affects Critical National Infrastructure in case of loss	Y/N	*List CNI supplied with power from this substation*
3.	Critical element in electrical grid capacity	Y/N	*List impact on electrical grid capacity due to loss*
4.	Loss cannot be compensated within 12 hours for critical loads	Y/N	*List the other substations that have adequate capacity & connectivity to compensate for loss*
5.	Loss of function/capacity results in > 75% reduction in supply capacity in its service area	Y/N	*List supply capacity reduction*
6.	Full time operational staff on site	Y/N	*List staff functions*
7.	Contains Grid Operations Control Facility	Y/N	*List Grid OCF functions and covered sites*
	Class B		
1.	Directly impacts hydrocarbon exports	Y/N	*List critical hydrocarbon facilities supplied with power from this substation*
2.	Minor impact on Critical National Infrastructure	Y/N	*List CNI supplied with power from this substation*
3.	Very important element in electrical grid capacity	Y/N	• *List impact on electrical grid capacity due to loss* • *List major critical loads supplied*
4.	Loss of function/capacity cannot be compensated within 24 hours for critical loads.	Y/N	*List the other substations that have adequate capacity & connectivity to compensate for loss*
5.	Loss of function/capacity results in > 50% supply capacity reduction in its service area	Y/N	*List supply capacity reduction*

	Class C		
1.	Important element in supporting the electrical grid capacity	Y/N	• *List impact on electrical grid capacity due to loss* • *List major critical loads supplied*
2.	Loss of function/capacity cannot be compensated for by other substations	Y/N	*List the other substations that have adequate capacity & connectivity to compensate for loss*
3.	Loss of function/capacity results in >25% supply capacity reduction in its service area	Y/N	*List supply capacity reduction*

	Class D		
1.	Loss of function/capacity results in >15%<25% supply capacity reduction	Y/N	*List supply capacity reduction*
2.	Remote support facility to other substations.	Y/N	*List other substations supported*

	Class E		
1.	The design of this substation consists of standalone building/buildings located in residential/commercial areas, within or near facilities/compounds.	Y/N	*List location and load supplied*
2.	Security countermeasures are dependent on location evaluated during the TSR/SVA	Y/N	*List CNI supplied with power from this facility*
3.	Security countermeasures provided by the FO	Y/N	*List FO recommended countermeasures*

نسخة من حصة لشركة المياه الوطنية

6 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 1 or Stage 3 workflow (as specified), to demonstrate how the FO is complying with specific requirements in this directive.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-17 Reference	Requirement	FO Response
1.	5.2.	FC Basis	*Provide TSR/SRA*
2.	5.4.	FC BCA Worksheet	*Provide worksheet with supporting documents*

نسخة مرخصة لشركة المياه الوطنية

نسخة من رخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-18

Security for Industrial Cities

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issued	Effective Date
1	Version 1.0	1438 / 2017	• 05 Sha'aban, 1438 • May, 01 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1. PURPOSE 7
2. SCOPE 7
3. ACRONYMS & DEFINITIONS 7
4. REFERENCES 7
5. GENERAL REQUIREMENTS 8
5.1 Risk Assessment 8
5.2 Perimeter 8
5.3 Fence Penetrations 8
5.4 Automatic License Plate Recognition 8
5.5 Intrusion Detection 8
5.6 Access Control 8
5.7 Common Requirements 9
5.8 Project Workflow 9
6. PROOF OF COMPLIANCE (POC) 9

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

The document provides specific security requirements for security at Industrial Cities.

2 Scope

This directive provides Facility Operators (FO) with specific security requirements for implementation at Industrial Cities.

3 Acronyms & Definitions

ACS	Access Control System
ALPR	Automatic License Plate Recognition
DA	Designated Authority: The owner or operator having jurisdiction over the industrial city.
FSC	Facility Security Classification
HCIS	High Commission for Industrial Security
PIV	Personal Identification Verification
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory requirement
SRA	Security Risk Assessment
VASS	Video Assessment & Surveillance System

4 References

This directive adopts the latest edition of the references listed.

SEC-01	*General Requirements for Industrial Security*
SEC-02	*Security Fencing*
SEC-03	*Security Gates*
SEC-05	*Security Systems at Industrial Facilities*
SEC-08	*Security Communications & Data Networks*
SEC-11	*Identification Cards*
SEC-14	*Security Project Management*
SEC-15	*Security Management at Industrial Facilities*

نسخة من خطة إدارة المدار الوطنية

5 General Requirements

Industrial cities are areas where a large number of autonomous industrial facilities are located in an area under the jurisdiction of a designated authority.

5.1 Risk Assessment

A SRA shall be carried out as stipulated in SEC – 01 & SEC 15 to determine the security systems that are required to maintain security at the facility perimeter and within the city. HCIS shall provide city specific security requirements where needed.

Each autonomous industrial facility within this industrial city shall comply with HCIS requirements and follow normal HCIS workflows.

5.2 Perimeter

The outer perimeter of an industrial city shall be fenced with a category 4 fencing system as specified in SEC-02. This fencing system shall be enhanced as specified in this document. Higher category fences shall be installed if required by the SRA or HCIS.

5.3 Fence Penetrations

Fence penetrations of the industrial city perimeter shall comply with SEC-02.

5.4 Automatic License Plate Recognition

Automatic License Plate Recognition systems, as specified in SEC-05, shall be installed to cover each lane at all entrances to the Industrial city.

5.5 Intrusion Detection

DA shall deploy SEC-05 compliant VASS systems, including long range detection systems, along the facility perimeter as specified in SEC-05 and at gates as specified in SEC-03.

5.6 Access Control

DA shall implement a SEC-05 compliant ACS to manage access into the city. PIV cards issued to personnel shall be fully compliant with SEC-11.

5.7 Common Requirements

This section describes requirements common to all Industrial Cities.

5.7.1 The specifications for each security system, sub-system and component shall comply with the requirements of HCIS SEC 01 – 20 where applicable.

5.7.2 DA shall ensure that a proper traffic study is conducted as part of the SRA to determine the amount of entrances/exits and the amount of lanes needed at each entrance/exit to manage vehicles and pedestrians.

5.7.3 City perimeter gates shall be structured as follows:

- Employee only
- Visitor/Contractor only
- Truck only

The traffic study shall determine the number of lanes required at each gate.

5.7.4 The operator of the industrial city shall implement a Security Control Center (SCC), as specified in SEC-05, to manage the city security environment.

5.8 Project Workflow

All security related work undertaken in the city shall follow the HCIS Project Workflow as stipulated in SEC 01.

6 Proof of Compliance

The proof of compliance as specified in each SEC Directive applicable in the security design of the city shall be submitted as PoC.

نسخة من مخططات شركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia

SEC-19

Residential Compounds for Industrial Facilities

Version 1.0

Security Directives
for Industrial Facilities

2017

نسخة مرخصة لشركة المياه الوطنية

KINGDOM OF SAUDI ARABIA
MINISTRY OF INTERIOR
HIGH COMMISSION FOR INDUSTRIAL SECURITY

RESTRICTED
All Rights reserved to HCIS. Copying or distribution prohibited without written permission from HCIS

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Version History

Item	Description	Issue Date
1	Version 1.0	• 5 Rajab, 1438 • 2 April, 2017

This Security Directive supersedes all previous Security Directives issued by the High Commission for Industrial Security (HCIS), Ministry of Interior.

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 PURPOSE 7

2 SCOPE 7

3 ACRONYMS & DEFINITIONS 7

4 REFERENCES 7

5 GENERAL REQUIREMENTS 8

5.1. COMPOUND DEFINITION 8
5.2. OTHER HCIS REGULATIONS 8
5.3. SECURITY INFRASTRUCTURE 8
5.3.1. Perimeter Boundary 8
5.3.2. Gates 9
5.3.3. Lighting 9
5.4. SECURITY SYSTEMS 10
5.5. FIRE PROTECTION 10
5.6. PROCEDURES 10

6 PROOF OF COMPLIANCE 11

نسخة مرخصة لشركة المياه الوطنية

نسخة مرخصة لشركة المدينة الوطنية

THIS PAGE INTENTIONALLY LEFT BLANK

1 Purpose

This document provide requirements for security of residential compounds at industrial facilities.

2 Scope

This directive provides Facility Operators (FO) with specific security requirements for implementation at residential compounds for industrial facilities.

3 Acronyms & Definitions

FO	Facility Operator: the owner, operator or lessee of a facility
HCIS	High Commission for Industrial Security
RWM	Rigid Welded Mesh
SCC	Security Control Center
Shall	Indicates a mandatory requirement
Should	Indicates an advisory requirement

4 References

This directive adopts the latest edition of the references listed.

HCIS/MOI	*Safety and Security Requirements for Residential Compounds & Residential Compound Evaluation Form*
SAF-06	*Plant Layout, Spacing and Access*
SEC-01	*General Requirements for Industrial Security*
SEC-02	*Security Fencing*
SEC-03	*Security Gates*
SEC-04	*Security Lighting*
SEC-05	*Security Systems at Industrial Facilities*
SEC-06	*Security Devices*
SEC-08	*Security Communications & Data Networks*

5 General Requirements

Residential compounds for industrial facilities shall not be constructed within the operational area perimeter of the industrial facility. FO shall use the requirements stated in SAF-06 to determine the minimum distance the residential compound perimeter shall be located from the operational area perimeter.

5.1. Compound Definition

Facility Operator shall provide HCIS with the following details for a proposed residential compound:

- Location
- Compound size (m2)
- Number of residential units
- Type (Family/bachelor)
- Tenant demographics (nationality)

HCIS shall advise FO of any additional security requirements, beyond the requirements stated in this directive that may be required.

5.2. Other HCIS Regulations

The requirements stated in the HCIS regulation entitled “Safety and Security Requirements for Residential Compounds & Residential Compound Evaluation Form” shall be implemented in conjunction with this directive. This regulation is available from HCIS on request.

5.3. Security Infrastructure

Security infrastructure for the compound shall incorporate the following elements as a minimum:

5.3.1. **Perimeter Boundary**

FO may use fencing or solid walls for the perimeter boundary. Where fencing is used the fabric shall be rigid weld mesh as specified in SEC-02.

The perimeter boundary shall be topped with barbed wire as specified in SEC-02. The perimeter shall be a minimum of 3m in height.

A 6m clear zone shall be located on both sides of the fence. The clear zone refers to an area, adjacent to the perimeter boundary, cleared of all

نسخة مرخصة لشركة الحماية الوطنية

vegetation & obstructions and maintained in this state. It shall be graded to direct water away from the boundary.

5.3.2. Gates

Gates leading into the facility shall incorporate the following elements:

- Gatehouse: Gatehouse shall use ballistic protection for the structure, windows and doors as specified in SEC-03.
- It shall be constructed in the center of the main gate, between the entrance and exit lanes.
- Anti-Vehicle Barriers: AVB's shall be installed in all exit and entry traffic lane as specified in SEC-03. AVB's shall be rated as specified in SEC-06.
- The approach to the gate shall utilize a VASM to manage approach vehicle speed as specified in SEC-03.
- The traffic management design shall incorporate an inspection/ rejection lane where vehicles denied access shall be either able to turn around without entering the facility or where suspicious vehicles can be inspected properly before allowed entrance.
- The rejection lane turning radius shall be sized for the largest vehicle expected to enter the facility. The inspection lane/turning point shall be located before the gatehouse.
- An auxiliary gate shall be installed as per SEC-03 requirements.
- A visitor management facility shall be established prior to the gate area to process visitor access authorizations.
- Specific measures shall be put in place at the gate to manage pedestrian traffic.
- Personnel access to the compound shall be controlled with turnstiles controlled by an access control system as specified in SEC-03.
- A toilet facility for gate personnel shall be provided as stipulated in SEC-03.

5.3.3. Lighting

The perimeter boundary, gate area and internal facility areas shall be adequately illuminated with area lighting systems as specified in SEC-04.

5.4. Security Systems

A VASS compliant surveillance system shall be deployed along the facility perimeter and at the facility gates.

5.4.1. If large areas inside the facility are not developed then VASS cameras shall be deployed to monitor this area.

5.4.2. All video imagery shall be analyzed by a video analytics system that shall annunciate an alarm at the gatehouse and/or local SCC.

5.4.3. All video imagery shall be recorded for 30 day period.

5.4.4. VASS systems and components shall comply with SEC-05 requirements.

5.5. Fire Protection

Fire protection system at the residential compound shall fully comply with applicable fire and safety industry standards for fire detection, alarm annunciation and suppression.

5.6. Procedures

FO shall compile proper security policy and procedures for the access control of all personnel, including contractors that need access to the compound.

FO shall have a complete set of procedures that include post orders, patrols and emergency response scenarios to manage compound security.

Communications to other IS assets shall be provided as specified in SEC-08.

نسخة مرخصة لشركة المياه الوطنية

6 Proof of Compliance

FO shall provide HCIS with a Proof of Compliance (PoC), as part of the Stage 3 workflow, to explain and demonstrate how the FO is complying with specific requirements in this directive. This will augment the Stage 3 submission which covers all items.

This PoC shall provide details for each of the requirements listed below. PoC submissions shall be supported with manufacturer's brochures or catalogs ONLY where they are relevant to the response.

In all cases the responses shall be specific in nature and include adequate technical details to demonstrate compliance to HCIS:

	SEC-19 Reference	Requirement	FO Response
1.	5.1	Compound Definition	*Provide requested details*
2.	5.3	Security Infrastructure	*Provide details*
3.	5.4	Security Systems	*Provide details*
4.	5.5	Fire Protection	*Provide overview of fire protection design*
5.	5.6	Procedures	*Provide a list of procedures for security personnel at the compound*

نسخة من شركة المياه الوطنية

نسخة مرخصة لشركة المياه الوطنية

Ministry of Interior
High Commission for Industrial Security
Riyadh
Kingdom of Saudi Arabia